HILLHEAD HOUSING ASSOCIATION 2000

INFORMATION TECHNOLOGY SECURITY POLICY

Approved/last reviewed by Management Committee: 7 February 2018

Date due for review: February 2021

The information in this document is available in other languages or on tape/CD, in large print and also in Braille.
For details contact the Association on 0141 578 0200 or e-mail: 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۔

Hillhead Housing Association 2000 is an established user of Information and Communications 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, 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 on computers, transmitted across networks, printed out on written paper, sent by fax, stored on tape, CD or disk 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
- Confidentially 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 Data Protection Act
- 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 training will be available to all staff
- 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 virus control, 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.

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 staff of the Association, apart from Section 8 which applies to Committee Members within the Association that may have limited access to the systems or information via email. However, Committee Members may find the other sections informative.

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. 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 Corporate Services Manager. Keep a copy for your own reference.

2.4 Non compliance of the IT Security Policy will be dealt with in accordance with the conditions of service disciplinary procedures.

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, staff 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 currently has 3 Servers. A Windows 2008 R2 server runs all the Association's files and general information. There is a separate print server and a smaller server hosts the Association's calendar. There is a Linux Server which runs the Association's integrated housing management, maintenance and finance systems.
- All data that is relevant to the business should be stored on the Server – G: Drive. This is in order that authorised staff may access it from the network and also to aid recovery in the event of data loss(Staff should never store data on their individual C: Drives)
- Employees (Users) will have access to a user group that is relevant to their needs of Data access rights as prescribed by the Corporate Services Manager / Admin.
- A modern, flexible internal network is used to connect the Servers, PCs and printers etc. to each other. 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 the Internet and e-mail.
- Each employee will have access to a PC 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 IT Equipment are permanently marked with a unique reference number and name and address of the Association
- The Asset Register is periodically reconciled to actual items held
- Procedures for the safe and secure disposal of redundant IT equipment are in place and ensure that all confidential data has been removed prior to disposal

Workstation Hardware units are replaced every 3 years and server hardware units are replaced every 4 years.

Security

3.4 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 and stakeholders confidence by meeting all obligations under the Data Protection Act 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.

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 customers the Association must protect its own internal systems. This is achieved by the following:-

    - All staff using IT systems will undergo basic training before using any system. This will include logging on and off, network locations for saving files, Anti-Virus protection, security risks and precautions and location of the IT procedures. This training will be organised by the Corporate Services Manager.
    - All staff must ensure that their passwords are confidential
    - Passwords should not be guessable words such as real names, date of birth, car registration etc. Passwords should preferably include a combination of upper and lower case and numbers. The Corporate Services Manager shall retain in a secure place a list of logon passwords to enable sharing of PCs for job share staff. Staff should not divulge their password to anyone else.
    - However there may be rare occasions that it may be absolutely necessary to do so for the operations of the business to continue or during system upgrades etc. In these cases the member of staff should advise the Corporate Services Manager.of their actions and their password should be reset at the earliest opportunity after the event.
    - If staff leave their computer unattended for any length of time they should either use the locking facility, use a screensaver password or log off the PC. Staff should always ensure that the PC they have been using is switched off, or locked if accessing remotely, before leaving the office.
    - Servers, PCs and laptops will be protected by Anti-Virus software (see section on anti virus Precautions below)
    - Software will be updated with any service/packs/patches/fixes available that correct any security issues. These updates will be carried out by the IT Consultant directly, remotely from a server or by instructing staff to install them. Staff must carry out these instructions within any timescales given.

- Any external access over public networks will be protected by the use of a Firewall
- Where third parties have access to the Association's systems, such as the IT consultant, Development Agents, Finance Agents, a contract or disclaimer must be obtained that will protect the information held and the integrity of the systems. 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 consultants 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 not encouraged and is viewed as a privilege and not as 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 as laid out in the Employment Conditions. The Association has the right to monitor the content of files and data located on any of the servers, PCs, notebooks, PDAs, removable media etc.
- Staff will be responsible for the security of all the Association's information that they take off site. This may be done on ~~Stick~~ removable media storage devices or via email. Staff should ensure that that any Association information held or transferred in this or similar manner is password protected.
- If staff store any information at home they should ensure that it is held securely and any information stored on their own PC/notebook etc is password protected or in a password protected area of their system.
- In order to facilitate recovery in the event of a failure to protect Association information:-

  a) The Director will prepare a Business Continuity Policy
  b) A full system back up of the servers will be completed each work day
  c) All data files shall be backed up on a daily basis. In order to make this effective it is vitally important that users save all Association information to a network server (any data stored on a local C:/drive will not be backed up)
  d) Back up drives will be secured in a fire proof safe
  e) Restorations of the back up drives will be tested at least once a month.

  Further information on IT Recovery can be found within the IT Disaster Recover Plan (Appendix 3)

Anti-virus precautions

3.5 The Association acknowledges that the threat of computer viruses, worms and Trojans. As a result anti-virus and Anti Malware software is installed on all PCs notebooks, as well as the Windows 2008 R2 server. All PCs and servers are configured to update their anti-virus protection automatically, with periodic manual checks being undertaken.

3.6 All PCs and notebooks are configured to update automatically on a daily basis and also to perform start-up scan on each reboot. They are also configured to scan e-mail and internet activity. However, staff cannot rely on the anti-virus software and should be vigilant for any signs of a virus. If a virus attack or contamination is suspected, it should be brought to the attention of the Corporate Services Manager. or Director immediately.

3.7 No External Devices (HDD, Memory Sticks et al) from any third party are allowed to connect to the network in the interest of Data Security.

IT Support

3.8 The Corporate Services Manager.and IT Consultant provide the support service for all IT related issues, although it is acknowledged that staff also provide a level of support amongst themselves.

3.9 The Corporate Services Manager.and 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 the IT Consultant; see appendix B “External Contacts” Users should gather as much information as possible about the fault before reporting it, e.g. details of equipment the problem occurred on, operating system of PC in question, applications being used, sequence of events that led to failure etc.

3.10 Each PC has a standard pre-set configuration which should not be amended by the user. Users should not install any software unless authorised by the Corporate Services Manager.or Director. Staff shall not move, relocate, reassign or otherwise modify hardware without notifying the Corporate Services Manager.. This will ensure that the Association’s assets are being managed and tracked effectively.

Training

3.11 The Association will recruit staff with the basic skills necessary. Additional training, including on the job training will be provided from the training budget.

4. Mobile Equipment

4.1 The Association has items of equipment that by their nature are mobile, such as laptops and digital cameras. Such equipment will be held by the Corporate Services Manager. Any request for an item of equipment must be made to the Corporate Services Manager before it is taken, in order that the whereabouts of the equipment is known at all times.

4.2 When in possession of such equipment, the member of staff must take care in regards 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. If equipment requires to be taken outwith the United Kingdom then the member of staff should seek the advice of the Corporate Services Manager. Some members of staff who work out of the office on a regular basis may be allocated a notebook as part of their role within the Association.

5. E-mail

5.1 E-mail (electronic mail) is a widely used form of communication within the Association and is used both internally and externally.

Purpose of e-mail

5.2 The objective of this section is to help the Association and its staff achieve the maximum benefit, at the lowest risk, from its use. The Association has provided e-mail to facilitate communication among its employees, Committee members and third parties such as business partners and suppliers. The e-mail system is the property of the Association and is intended 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.

Guidance on legal issues

5.3 E-mail users should be aware of the following

- External e-mails are Association records
- E-mails have the same legal status as other mailed documents
- Courts can order that e-mail messages are made available
- Any information held on individuals, including that in the e-mail system, may be subject to the terms of the Association's Data Protection Registration
- If in doubt, ask the Corporate Services Manager 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 e-mails through the Association's systems. Staff should be aware that this will also cover e-mails marked or considered private, confidential etc.

Information Confidentiality

5.5 E-mail is an inherently insecure system (a bit like sending information on a postcard). 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 e-mail then it should be done through an attached file that is password protected, with the password notified to the recipient by a phone call.

5.6 Secure e-mail is unavailable at present.

Drafting of E-Mail

5.7 It is the Association's policy to ensure a consistent standard of e-mails issued. To that end, users should:-

- Draft e-mails carefully, taking into account discrimination, harassment, Association presentation and defamation issues.
- All employees should use suitable e-mail etiquette at all times. See Appendix B.
- Not attach large files to e-mails. If internal, these will contribute to the disk space allocated to both the sender and recipient. A link or note of where the file is stored should be used instead. If the e-mail is external you should remember that the recipient may only have a modem link and large files will take a long time to be downloaded. A limit may be set on the maximum message size that can be sent or received through the system.
- External e-mails should have the confidentiality clause appended.

5.8 The confidentiality clause is included in the email appendix below:

++++++++++++++++++++++++++++++++
<Name of Employee>
<Job Title>
Hillhead Housing Association 2000
2 Meiklehill Road
Hillhead
Kirkintilloch
G66 2LA
Direct Dial: <enter ddi for employee>
Tel: +44 (0) 141 578 0200
Fax:+44 (0) 141 578 0201

Hillhead Housing Association is a recognised Scottish Charity SC 029908

Disclaimer: This email may contain confidential information which is intended for the required recipient only. If you are not the named recipient you should not take any action in relation to this email , other than to notify us that you have received it in error. If this email contains attachments you should ensure that they are checked for viruses before opening them.

please consider the environment before printing this e-mail.
++

Virus Threat

5.9 E-mails offer a path for viruses to contaminate the Association's systems, through the e-mail itself or an attached file. The e-mail system has Anti-Virus protection but users are reminded of the danger, (see Anti-virus Precautions above).

5.10 However, staff should pay particular attention to e-mails that they did not expect to get even if they are from recognised senders. Many viruses can use e-mail addresses from an infected PC, making them appear to be from someone they know. Special consideration should be given to e-mails if they contain file attachments, especially if the file extension is '.exe', '.scr', '.pif' etc. or they apparently contain a double file extension e.g. '.doc.exe'. These examples are in no way exhaustive.

5.11 If a member of staff is suspicious of an e-mail they have received they should contact the Corporate Services Manager immediately. It should be noted that the server or e-mail software may 'filter out' some file attachments that are considered dangerous.

5.12 The Corporate Services Manager will alert staff of any major virus threats that are prevalent at that time. Staff should always take heed of any warnings and carry out any security updates if advised.

Time Management

5.13 While the e-mail 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 e-mail messages that restrict the interruptions.

5.14 The e-mail server receives messages from Association's Internet Service Provider every 15 minutes during the working day, while internal messages are delivered immediately. E-mails sent from the Association are done so near-instantaneously, but staff should be aware that their arrival will depend on other various systems.

Personal Use

5.15 Personal use of the e-mail system is not encouraged. It is preferable that Staff should not read, compose or send personal emails during flexible working hours. If necessary this should be done in an individual's personal time. If any member of the management team perceives any abuse of personal use in privileges the individual's email account will be subject to an audit and the individual may be subject to disciplinary action. Best practice is that any personal emails should be deleted after reading or sending.

Retention Policy

5.16 Most e-mail 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.

5.17 Retention and deletion of old e-mail messages should be managed by each employee bearing in mind data storage levels, archival records, contractual evidence and legal requirements. Unless e-mails 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:

- Saved as a file in the appropriate folder on the Network Server

OR

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

5.18 Mail is local to each machine.

5.19 Staff will be allocated a certain amount of disk space on the server where all the information from their Outlook, including e-mail, will be stored. Staff will have to perform regular housekeeping of saved messages, including deleting copies of "sent items" and "deleted items" as well as other Outlook features, in order that they stay within their limit.

5.20 An e-mail will be sent automatically by the system advising the member of staff 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 e-mails.

Inappropriate Use

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

- The unauthorised distribution (internally or externally) of information known or believed to be confidential
- Representation of personal opinions as that of the Association
- Concealment or misrepresentation of names or affiliations in e-mail messages
- Alteration of source or destination addresses of e-mail
- Use of e-mail facilities for commercial or private business purposes
- Use of e-mail which unreasonably interferes with or threatens other individuals
- 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

5.22 Both Association and staff must accept the risk that inbound e-mail 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 Corporate Services Manager 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 Cable (Broadband) connection to all staff through any PC or notebook connected to the Association's network. In order not to disrupt work, users should keep on-line to a minimum.
- Normal use is restricted to the World Wide Web (www) and File Transfer Protocol (FTP) sites. Users should consider Internet activity to be public and not reveal confidential information.

- Access to Internet newsgroups and social networking sites is not permitted.
- The Internet should be used to access business related information only.
- Staff are discouraged from accessing personal hotmail or Google e-mail accounts from office PCs.
- 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 an anti-virus check.

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 Corporate Services Manager.. A staff sub group meets periodically to review and update content of the Website.

Virus Threat

6.6 The Internet offers a path for viruses to contaminate the Association's systems primarily by downloading or running infected files. The Association's systems have anti-virus protection and also a firewall provided through Windows 2008 R2 server but users are reminded of the danger (see anti-virus precautions above).

6.7 Staff should pay particular attention to the types of files available from a website and should only download mainstream files such as:

- Word (filename.doc)
- Excel (filename.xls)
- Acrobat (filename.pdf)

6.8 Under no circumstances should staff download or run any system updates, patches, fixes etc unless expressly instructed by the Corporate Services Manager. Staff 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 Corporate Services Manager.

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
- Hillhead Housing Association 2000 has provided a modern telephone system with the capacity for growth to meet requirements for the foreseeable future
- A Mitel 8528 system delivers telecommunications to each desk using the company's structured cabling system
- A single direct telephone line is available to use for outgoing calls in the event of a failure in the main telephone system (currently used for the fax).
- 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.
- Incoming calls will be answered with a standard, friendly greeting

Telecommunications Procedures

7.3 The following procedures should be followed when using the Association's Telecommunications facilities:

- Incoming telephone calls will be answered in a friendly manner using the following standard greeting, "Good morning/afternoon, Hillhead Housing Association 'Your Name' speaking".
- Incoming calls via the switchboard at the office which are not able to be answered will be diverted to voice mail.
- Direct Dialled numbers (DDI) or internal calls divert to Voicemail after seven rings, which gives the caller the options to leave a recorded message.
- Callers to busy extensions will receive the engaged tone, or a recorded voicemail message in which the caller is invited to leave a message.
- Only international calls will be barred at internal extensions; employees are expected to use their discretion when making long distance calls, and have regard to the potential cost and benefit to the business of such calls.
- Fully itemised billing will be used to monitor call charge expenditure.
- Users Voicemail messages should be checked and updated frequently and must always be relevant.
- The Telephone System's Auto-Attendant will be used to answer calls and take messages when the office is unmanned.
- A fax machine is located in the main office.
- Mobile telephones for essential out of office use are supplied by the relevant staff.

- Telephone System faults and requests should be directed to the Corporate Services Manager.

Personal Use

7.4 Personal use of the phone system and mobiles are not encouraged. Unless in an emergency staff should try not to make or take personal calls during flexible working hours.

8. Committee

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 normally be via e-mail but could also include any.removable media storage device. Committee members will not have direct access to the Association's systems.

Security

8.2 The security of information is of paramount importance and therefore it is the Association's policy to protect business information from all threats, internal and external, deliberate or accidental. It is equally important to maintain customer confidence by meeting all obligations under the Data Protection Act and any other relevant legislation.

Confidentiality

8.3 All the Association's information must be protected from unauthorised disclosure. This includes 'leaks' of information to third parties or to the media. It also includes unauthorised access to data and 'hacking' into systems from internal or external locations. Association Committee members will be responsible for the security of all the Association's information that they hold outwith the premises of the Association's office. This information may be held on any physical media storage device or via e-mail. This information may subsequently be held on their own PC/notebook. Committee members should ensure that any Association information held or transferred is secure, even from their family or friends that may also use their PC/notebook. Any information held on removable media devices should be stored in a secure place.

Anti-virus Precautions

8.4 If Committee members transfer any information back to the Association via e-mail, floppy disk etc they should take great care not to transmit any computer virus etc to the Association's systems. The Association highly recommends that the Committee members have anti-virus software and should be vigilant for any signs of a virus. If a Committee member suspects that they may have inadvertently transmitted a virus to the Association, they should bring it to the attention of the Corporate Services Manager of the Association immediately.

8.5 Hillhead Housing Association advise Committee members that all files from an external source eg those arriving via any removable media device, e-mail or the Internet should be checked for viruses BEFORE used in any way.

E-mail

8.6 E-mail is now a widely accepted form of communication and is increasingly being used between staff and Committee members. However, Committee Members should be aware of the following issues that apply to any e-mail that concerns Association business as well as more 'personal' e-mails to staff eg jokes.

Guidance on Legal Issues

8.7 Users should be aware of the following:

- External e-mails are Association records
- E-mails have the same legal status as other mailed documents
- Courts can order that e-mail messages are made available
- Refer to existing guidelines on safeguarding confidential or competitive information
- Any information held on individuals including that in the e-mail system may be subject to the terms of the Association's Data Protection Registration

Privacy

8.8 In order to protect the Association from legal, regulatory or other repercussions, Committee members should be aware that Hillhead Housing Association 2000 may monitor the content of incoming and outgoing e-mails through the Association's systems. This will also cover e-mails marked or considered private, confidential etc.

Information Confidentiality

8.9 E-mail is an inherently insecure system (a bit like sending information on a postcard). 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 e-mail then it should be done through an attached file that is password protected with the password notified to the recipient by a phone call.

8.10 The Association currently do not use any encryption on e-mail at present.

Drafting of E-mail

8.11 It is Hillhead Housing Association's policy to ensure a consistent standard of e-mail messages emanating from the Association. To that end, users should

- Draft e-mails carefully, taking into account discrimination, harassment, representation and defamation issues
- All Committee members should use suitable e-mail etiquette at all times. See Appendix B
- Not attach large files to e-mails as the recipient may only have a modem link that would take a long time to be downloaded

Virus Threat

8.12 E-mails offer a path for viruses to contaminate the Association's systems and the Committee members own PC/notebook through the e-mail itself or an attached file. As stated in section above, the Association highly recommend that the Committee members PC/notebooks have anti-virus software installed.

8.13 They should pay particular attention to e-mails that they did not expect to get even if they are from recognised senders. Many viruses can use e-mail addresses from an infected PC, making them appear to be from someone they know. Special consideration should be given to e-mails if they contain file attachments, especially if the file extension is '.exe', '.scr', '.pif' etc or they apparently contain a double file extension eg '.doc.exe'. These examples are in no way exhaustive.

Retention Policy

8.14 Most e-mail 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.

8.15 Retention and deletion of old e-mail messages should be managed bearing in mind data storage levels, archival records, contractual evidence and legal requirements. Unless e-mails 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:

- Securely saved on their PC/notebook

or

- Printed in hard copy which shall be retained as the 'official record'

or

- Forwarded to the Association for retention on their systems

8.16 Committee members should perform regular housekeeping of saved messages including deleting copies of 'sent items' and 'deleted items'.

Inappropriate Use

8.17 Hillhead Housing Association 2000 prohibits the use of the Association systems to carry inappropriate material, in particular:

- The unauthorised distribution (internally or externally) of information known or believed to be confidential
- Representation of personal opinions as that of the Association
- 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

8.18 Committee members must take this into consideration when e-mailing anyone regarding Association business or contacting staff.

Appendix A

Employee Agreement

Each employee must confirm that they have read and understood the contents of Hillhead Housing Association 2000's Information and Communication Technology 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 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 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 removal from the Management Committee.

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

Date: ……...

Signature: ……

External Consultant/Third Party Agreement

All external consultants/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 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 Technology Security Policy.

Date: ……...

Signature: ……

Company:……

Appendix B

USE OF EMAIL

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

Courts have the power, in some circumstances, to order that e-mail messages be available for open inspection. The same standard of care should, therefore, be exercised in the content of an e-mail message as in any other business communication.

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

Consider the various communications e-mail may replace:

- Telephone messages
- Scribbled notes
- Memos
- Letters

Then remember that your e-mail 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 e-mail 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 e-mail. 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 and fax numbers as well as the address of the main office is contained in the automatic confidentiality clause.
- Write in mixed case. Upper case counts as SHOUTING.
- Use correct spelling and grammar
- Use ‘smileys’ eg ☺ 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 e-mail message so use ☹ ☺ ;-) and the other 101 variants of ‘emotions’ to help express emotion.
- Use an e-mail 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 e-mail message in anger – it will get there very fast and you may regret it!
- Never assume that people have read their e-mail 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 e-mail covering multiple topics. Send several short e-mails each covering a single topic and then it is easy for people to respond.

Appendix C

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 Technology in the event of such incidents. Implementation of the recovery measures here will be the responsibility of the Corporate Services Manager who will liaise as necessary with the Association's IT consultant.

The Association's insurance policy allows for replacement of equipment and the amounts of cover are:

Computers	£50,000
Portables, including laptops	£3,500
Presentation Equipment (including mediascape equipment)	£4000

2. Back Up System

All data on the main servers is backed up (full image backup) on a daily basis with this back up being stored outwith the office overnight. Remaining Drives will be stored within the Association's fire proof safe. It is the responsibility of the Association's Finance Officer (or Finance & Corporate Customer Services Assistant in his absence) to undertake this task.

3. Disaster Scenarios

Outlined below are foreseeable disaster scenarios which this plan will cover.

3.1 Server Unavailable

Where the server is unavailable through theft, damage, the Corporate Services Manager will liaise with the IT Consultant in order to facilitate the installation of the off-site redundant server to be loaded and installed in place of the affected server within 48 hours.

3.2 Loss or Corruption of Data

Where there is loss or corruption of data caused by a software bug or virus or another form of malicious or accidental intervention, all systems can be restored from program disks and the latest available back-up tape. Copies of all main server software and desktop programs are held in the fire proof safe as well as copies held off-site with the IT Consultant. Depending on the severity of data loss or corruption, recovery would take between one and five days.

3.3 More than one server unavailable

In the event of failure, theft or damage to one or more servers, the IT Consultant will determine the severity of damage and ascertain the necessary replacement timescale. All computer hardware is maintained under manufacturer's warranty. Any data lost can be restored as outlined above.

In the event that a Server cannot be repaired or has been stolen, the IT Consultant would arrange for a replacement to be ordered. Complete set up and recovery may take up to ten working days.

3.4 Entire Network Unavailable

Where the entire network is unavailable due to failure of cabling and/or network switches/hub, this issue would be addressed by immediately contacting the IT Consultant to repair or replace equipment as necessary.

It is envisaged that permanent recovery of the switches and cabling could be effected within five working days, yet recovery of the full network may take up to ten working days.

Business continuity can be maintained within 24 hours through purchasing replacement switches and network cables, arranged with the IT Consultant who will also set up a temporary network to allow normal functionality to be rolled out to a limited user base.

3.5 Complete unavailability of all IT Equipment

This may occur through severe damage to the office in fire, flood etc.

On day one of the disaster, an assessment will be made of how long it is likely to be before the offices are usable. The IT Consultant will be notified and complete replacement of equipment and systems timed to fit in with recovery of office accommodation.

Alternative accommodation will be arranged in accordance with the Association's full Disaster Recovery Plan, and the IT Consultant will arrange for a temporary network to be supplemented with additional equipment until the Association's full network capability is restored.

4. Responsibility

In the event of a serious incident, disaster recovery activities for IT will be co-ordinated by the Director and Corporate Services Manager in liaison with the Association's IT Consultant.