E-Mail & Internet Policy

Serving Inverclyde since 1968

www.clochhousing.org.uk

ClochHA ClochHA

1. Definitions

Throughout this policy the term “Association” will relate to Cloch Housing Association (CHA), “governing body” relates to CHA’s board.

2. Introduction

Electronic mail and the Internet has greatly facilitated internal as well as external communication throughout the world. Unfortunately, this communication tool also has the potential for misuse.

To clarify the Associations policy on the use of E-mail and the Internet, we have developed this policy statement.

Unnecessary or unauthorised Internet and E-mail usage can cause network and server congestion. It can slow other users, take away from work time, consume supplies, and tie up printers and other shared resources.

Unlawful Internet and E-mail usage may also bring negative publicity for the Association and expose the firm to significant legal liabilities.

The Association must take special care to maintain the clarity, consistency and integrity of the Associations corporate image and position. Anything any employee or governing body member writes in the course of acting for the Association on the Internet can be taken as representing the Association’s corporate position.

3. Coverage

This policy applies to all employee and board members of the Association and refers to all E-mail and Internet resources in the Association.

Individual departments and may define additional "conditions of use" for Internet and E-mail facilities under their supervision. Any such additional conditions must be consistent with this overall policy but may include more detailed guidelines and, where necessary and appropriate, additional restrictions.

Any person who uses the Associations Internet and E-mail facilities consents to all of the provisions within this policy and agrees to comply with all of its terms and conditions and with all applicable laws and regulations.

Any user of the Internet and E-mail system, whose actions violate this policy, or any other Association policy or regulation, may be subject to limitations or elimination of electronic mail privileges as well as other disciplinary actions.

The policy aims to ensure that use of the Internet and E-mail among Association users is consistent with its own internal policies, all applicable laws, and the individual users’ job responsibilities.

The policy also aims to establish basic guidelines for appropriate use of the resources.

4. Access

It is the Associations intent as far as possible to provide network-connected E-mail and Internet facilities for the use of staff and governing body members. It is also the Associations intention to provide a communications link between its own E-mail system and the mail systems that operate on the national and international data networks.

The primary purpose of such access is to encourage greater business efficiency and to enhance knowledge, learning and communication opportunities for the Association as a whole and its people as individuals.

Occasional personal Internet access and incidental social communications using E-mail are not disallowed by this policy and are permitted so long as this does not interfere with the performance of expected duties. The Association and its ICT support provider reserves the right, via specialised web filtering software, to block certain categories of internet sites. Each user should comply with specific policies of their individual unit/section/department.

A manager concerned about an employees' potential violation of their ICT usage (for example, excessive use of electronic mail for personal use or spending large quantities of time on social media) should NOT unilaterally seek to gain access to a users' electronic communications. Instead, the manager should:

- Review whether or not expectations and standards in this area have been well communicated and made clear to the user.
- Pursue direct communication with the user regarding the issue.
- Proceed as one would handle any personnel-related disciplinary action.

In general employees may use their Internet and E-mail facilities for business related purposes, non-business research or browsing during mealtime or other breaks, or outside of work hours, provided that all other usage policies are adhered to.

Where staff have been authorised to work from home and authorised to access the Associations network remotely all standards within this policy should be adhered to.

The Association provides employees access to the vast information resources of the Internet with the intention of increasing productivity. While the facility has the potential to help them do their job faster or smarter, there is justifiable concern that it can also be misused. This E-mail and Internet usage policy is designed to help staff and governing body members understand the Associations expectations for the use of those resources in the particular conditions of the Internet, and to help them use those resources wisely.

The Internet for this Association is a business tool, provided to users at significant cost. That means the Association expect staff and governing body members to use Internet access primarily for business-related purposes, (i.e., to communicate with customers and suppliers, to access Internet hosted software, to research relevant topics and obtain useful business information).

5. Proper Use

E-mail is a very informal medium. It is closer to speech than a written communication, and yet there is a permanent written record. It typically lacks the care given to a written communication, and can often be stilted, abbreviated conversational language with heavy use of “emoticons”.

In addition, it is often the case that people "say" things in E-mail and on-line which they might not otherwise feel comfortable communicating to others.

A combination of such informalities has the potential to create potentially dangerous situations such as, sending E-mail containing negligent misstatements or binding the organisation in other ways using E-mail to conduct harassment on colleagues or others.

E-mail seems to be a fairly common ingredient in workplace harassment cases and under existing anti-discrimination legislation, an employer can be liable for acts of his employees, whether or not done with the employers’ knowledge or approval.

The following general protocol is therefore intended to guide users on the Associations standards in these areas:

- External E-mail messages should have appropriate signature files and disclaimers attached.
- Users should be familiar with general housekeeping good practice (e.g. the need to delete E-mail messages regularly).
- Users should use appropriate etiquette when writing E-mail messages; the use of capital letters, for example, is considered to be the equivalent of SHOUTING.
- Inappropriate messages are prohibited including those which are sexually harassing or offensive to others on the grounds of age, disability, race, religion, LGBT or gender.
- If someone is the recipient of such messages they should raise their concerns with their manager immediately.
- Users also have the right to raise a grievance should they receive offensive E-mail or be concerned over a colleagues’ general use of the Internet/E-mail resources.
- Users should not send potentially defamatory E-mail messages which criticise other individuals or organisations.
- Users should not access or download inappropriate material, such as pornography, from the Internet.

- Users should take care not to infringe copyright when downloading material or forwarding it to others.

Some people will send an angry E-mail message; one that they would never say in person. Take a minute before entering into an E-mail conversation. Be careful about what words are used and how they are said. Remember that messages can be printed or forwarded. Do not say things that will be regretted later.

Users should conduct themselves honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as they would in any other business dealings.

All existing Association policies apply to conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of Association resources, discrimination, harassment, information and data security, and confidentiality. Examples include social media policy, data protection policy, business disaster recovery and ICT password policy.

Only those employees or officials who are authorised to speak to the media or in public gatherings on behalf of the Association may speak/write in the name of the Association to any newsgroup.

Other employees may participate in newsgroups in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this Association, the employee must refrain from any unauthorised political advocacy and must refrain from the unauthorised endorsement or appearance of endorsement by the Association of any commercial product or service not sold or serviced by this Association, its subsidiaries or its affiliates.

Only those managers and Association officials who are authorised to speak to the media or in public gatherings on behalf of the Association may grant such authority to newsgroup participants.

The Association retains the copyright to any material posted to any forum, newsgroup, or web page by any employee in the course of their duties.

Employees are reminded that newsgroups are public forums e.g. Facebook, where it is inappropriate to reveal confidential Association information, customer data and any other material covered by existing Association secrecy policies and procedures.

The Association will comply with reasonable requests from law enforcement and regulatory agencies for logs diaries and archives on individuals' Internet activities.

Employees with Internet access may not use Association Internet facilities to play games against opponents over the Internet.

Employees should schedule communications-intensive operations such as large file transfers, video downloads, mass e-mailings, etc. for off-peak times.

Any file that is accessed will be automatically scanned for malicious content such as viruses by Association security software before it is allowed to be downloaded.

Employees with Internet access may not upload any software licensed to the Association or data owned or licensed by the Association without explicit authorisation from the system administrator or manager responsible for the software or data.

If a user is at all unsure about proper use of Internet and E-mail facilities, they should ask for clarification or permission from their manager or a system administrator.

6. Improper Use

As mentioned earlier, the Association provides Internet and E-mail facilities to support its communication, learning and service activities and associated administrative functions. Any use of the facilities that interferes with these activities and functions or does not respect the image and reputation of the Association is therefore improper.

In general, policies and regulations that apply to other forms of communications at the Association also apply to Internet and E-mail usage.

In addition, the following specific actions and use of Internet and E-mail facilities are improper:

- 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.
- Use of E-mail that degrades or demeans other individuals – whether Association employees or others.
- 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 Association 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 is prohibited.
- The display of any kind of obscene image or document on any Association computing resource is prohibited. In addition, obscene material may not be archived, stored, distributed, edited, or recorded using Association network, printing, or computing resources.
- No employee may use Association facilities knowingly to download or distribute pirated software or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights.
- No employee may use the Associations Internet or E-mail facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program code or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
- The Associations Internet and E-mail facilities and computing resources must not be used to knowingly violate the laws and regulation of the United Kingdom or any other nation in any material way.

Some generic terms for much of the above are as follows and are expressly prohibited under this policy:

Spamming

Spam is broadly defined as unsolicited, E-mail sent to a large number of recipients, and its content is not Association business related. The Association's E-mail accounts are not allowed to be used for the purpose of sending SPAM messages. Not only is this a misuse of Association resources, but it can also result in external sites "black listing" the Association, prohibiting delivery of any future E-mails to our location.

Chain letters and Pyramid schemes

These E-mail messages are sent to a specific number of people, usually professing a "get rich quick" scheme. The recipients are then asked to forward the message on to the same number of people. These types of messages are illegal and not allowed on the Association network. Accounts found associated with chain letters or pyramid schemes may be turned off without warning.

Spoofing

Spoofing refers to someone sending mail that "appears" to be from someone else. This is the same as forging someone else's identity.

Harassment

Harassment via E-mail, as with other avenues of communication, is prohibited.

7. System Administrators

System administrators (sometimes known as Postmasters) have specific responsibilities and access capabilities. Because of these special access capabilities they are expected to exercise special care in order to protect the privacy of the individuals whose electronic communications they handle.

System administrators shall maintain the following standards:

- Use machine headers and machine-generated messages in order to return undeliverable mail.
- Avoid reading message content to the greatest degree possible.
- Inform users of procedures for providing service, and assiduously attempt to respect privacy.
- Inform users and be straightforward if something goes wrong, in order to maintain trust.
- Keep confidential the content of any message that was inadvertently read in the course of redirecting undeliverable mail.
- Consult with users first if it seems necessary to go beyond machine-generated explanations.
- Be informed about and follow Association policy regarding privacy in electronic communication.
- Configure software to apply restrictions on the size and type of files that may/may not be downloaded.

System administrators have a role in determining where on the security versus service continuum the Associations Internet and E-mail usage system resides. They must inform their users of the trade-offs between service and security that exist on their system.

System administrators will therefore need to take specific actions to ensure, to the greatest degree possible, that Association policy is followed and that users are informed about the degree of privacy of their communications.

The following list of information items will help users be as knowledgeable as possible about the systems that they use. It will also help system administrators manage the issues of electronic mail and privacy.

The IT Department and IT Support contractor will act as system administrators; sharing responsibility for the implementation and monitoring of this policy. The system administrators report to the leadership team.

System administrators will not routinely examine E-mail content or monitor Internet activity unless there are good reasons to suspect the system is being abused and the rules ignored.

8. Privacy

The Association has software and systems in place that can monitor and record all Internet and E-mail usage. Security systems are capable of recording (for each and every user) each web-site visit, each chat, newsgroup or email message, and each file transfer into and out of our internal networks, the Association reserves the right to monitor and record usage at any time monitor.

System administrators will review Internet activity and analyse usage patterns, and may choose to publicise this data to assure that Association Internet resources are devoted to maintaining the highest levels of productivity.

The Association reserves the right to inspect any and all files stored in all areas of its network and computer systems in order to assure compliance with policy and ensure the security of the Association.

Monitoring Procedure

1. The ICT Project Manager receives daily reports on attempts to access blocked websites, these are system generated by the web filtering software.

2. The ICT Project Manager will run internet usage reports for the Leadership Team to review if required

3. Any report showing excessive use of the Internet will prompt further detailed usage reports to be requested.

4. The detailed report will be reviewed to calculate actual usage time, excluding lunch breaks and annual/flexi leave and to identify if the sites visited were for business use or personal use.

5. Where it is found that there has been a high usage of internet to non-business sites the Section Head will be advised and steps to deal with this using the disciplinary procedure will be taken.

6. If the usage at step 2 is by the Leadership Team the Director will deal directly with this by implementing steps 3 to 4.

The Association uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites and may block access from within networks to all such sites.

If users finds themselves connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any web filtering policy, and report this site to the system administrator.

In general the Association's view on privacy issues is best set out by the answers to the following questions that are typically most often raised in this area:

a) What is unauthorised access to information resources in this regard?

Generally, a good guideline to follow is that authors or parties to E-mail should be the primary sources of authorisation in granting access to their information or files. Third party access to electronic mail ordinarily may only be accomplished through either the sender or the recipient(s) of that mail.

b) Is it possible to invade the privacy of individuals and if so is authorisation always required?

Since Association resources are being used to create and store files, users should understand that the Association must assign certain individuals responsibility for maintaining, repairing, and further developing those resources.

In the normal course of doing their assigned work some individuals, by virtue of their positions within the Association and their specific responsibilities, may have special access privileges to hardware and software and therefore to the content that resides in those resources.

The Association will strive to protect individual privacy by ensuring that the number of individuals with this level of access is strictly limited and that such individuals are selected for their judgment and ethics, as well as their technical expertise.

Such positions, and the individuals who hold them, will be governed through defined responsibilities and procedures. (See Section 9 below on system administrators)

c) How possible is it that electronic mail might be seen?

All users should be aware that E-mail may pass out of one machine environment, across a network, and into another totally different machine environment even within the Association itself.

This transport becomes increasingly complicated as mail travels between offices, regions and countries. Each time the information technology hardware, software, and service environment changes, the level of security may be affected.

In addition to differing security levels in different machine environments, electronic mail may also be compromised because of an individual's own difficulty in sending a message to an intended recipient.

The sender may be uncertain about remote addressing; the message may not be deliverable, and a rejection message may be generated.

If such rejections can be delivered to the original sender, ordinarily no person sees the message. If, however, the message can't be delivered to the original sender, systems can be configured to either pass the message to someone (a postmaster) for assistance or to discard the rejection without the sender knowing anything about the problem.

d) Who are the system administrators and what role should they play?

System administrators are individuals who have the specific duties of enabling undeliverable mail to reach its destination, handling other delivery problems, and answering user questions about mail travel.

Users should know that mail that is deliberately sent to system administrators for advice or mail that is undeliverable will be seen by others.

System administrators should therefore observe procedures and privacy standards analogous to those used by postmasters who receive letters in a post office.

e) What material may be retrievable if required by law?

Because systems on which users carry out their communications and computing vary widely, so too do back up and save procedures.

Users need to be informed about the back-up procedures in the environment in which they are working because those procedures will ultimately determine what information has been retained in the course of backing up the system and perhaps what may be accessible by others through legal means.

The Association will hold a deleted email for 14 days before it is irretrievable, however, within some system environments, a deleted or expired message will entirely disappear and be irretrievable after 28 days. In some environments senders may have the facility to override the automatic expiration of messages by specifying longer parameters.

Messages that become part of a forwarding or history chain may be retrievable longer. File save procedures in each environment determine what material is saved and in what form.

While Association system administrators will not monitor the contents of mail messages as a routine procedure, the Association does reserve the right to inspect, copy, store, and disclose the contents of electronic mail messages at any time.

However, it will do so only when it believes it is appropriate to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the electronic mail facilities.

Any system administrator who believes such actions are necessary must first obtain the approval of the Directorate or equivalent person.

9. Security

Security, including protection from viruses as well as security of Association information, is a concern with both Internet and E-mail use.

While a direct connection to the Internet offers a range of potential benefits, it can also open the door to some significant risks to data and systems if users do not follow appropriate security disciplines. This may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers.

The overriding principle is that security is to be everyone's first concern.

An Internet and E-mail user can be held accountable through the Associations disciplinary policy for any breaches of security or confidentiality.

The Associations policy statement on personal security is reproduced below:

- Users should keep personal log-on and passwords confidential and change passwords on a regular basis in compliance with the Associations password policy
- Failure to adhere to this policy jeopardises network security and puts users at risk of potential misuse of the system by other individuals.
- Network users may be held responsible for all actions taken using their personal network access permissions.
- In a further effort to ensure the security of our systems and the information placed on it by users, the Association has software that governs the downloading, and uploading of files.
- Virus detection software is installed on individual workstations and network servers. Users are responsible for virus checking of downloaded files.

If a user does not know how to do this or doesn't fully understand the conventions involved here they should seek advice from their manager or system administrator.

10. Legal Issues

Users should be aware of the following Acts of Parliament which are in place to protect both users and the Association.

a) The UK Data Protection Act 2018

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). More details can be found in section (b).

b) General Data Protection Regulation (GDPR) 2018

A regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU)

The GDPR set out to structure the way we collect, store, process and remove personal data, as well as ensuring we hold it securely and tell the customer what we are doing with their data.

- Data must be gathered by consent and only processed for the reasons stated by the Association.
- Data Subjects can request to have the processing of their data limited or indeed, their data removed, although each request is decided on a case by case basis.
- The Regulations require the Association to have Privacy Policy and appendices of a Fair Processing Notice for customers and staff and Data Sharing Agreements with contractors.
- Breaches in Data Security require to be reported to the Information Commissioner's Office within 72 hours.
- The Association must deal with requests by Data Subjects to see their personal data within 30 days and with no fee.

c) The Freedom Of Information (Scotland) Act (2002)

The Freedom of Information Act give everyone a right to access information held by Scottish Public Authorities (Note: not personal information). FOISA recognises registered social landlords as Scottish Public Authorities.

The Associations dedicated standalone policies provide detailed information on the above Acts and Regulations.

d) The Computer Misuse Act (1990)

The Computer Misuse Act protects personal data held by organisations from unauthorised access and modification.

The act makes the following illegal:

- Unauthorised access to computer material. This refers to entering a computer system without permission (hacking).
- Unauthorised access to computer materials with intent to commit a further crime. This refers to entering a computer system to steal data or destroy a device or network (such as planting a virus).
- Unauthorised modification of data. This refers to modifying or deleting data, and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information).
- Making, supplying or obtaining anything which can be used in computer misuse offences.

e) The Human Rights Act 1998

The Human Rights Act 1998, which, amongst other things covers the right to privacy, came into force in 2000. A UK citizen can assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

f) The Communications Act 2003

It is declared an offence to "persistently make use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety"

Sending malicious communication using social media is a criminal offence.

g) The Obscene Publications Act 1959

All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

A computer disk, including the principal hard disk of the computer, can constitute an obscene article for the purposes of this Act if it contains or embodies matter that meets the test of obscenity.

'Publish' has a wide meaning and is defined as including distributing, circulating and selling, giving, lending offering for sale or for lease.

It seems clear that material posted to a newsgroup or published on the World Wide Web page falls within the legal definition of publishing and is

therefore covered by the Act. The publisher would appear to be the originator or poster of the item.

h) Protection of Children Act 2003; Criminal Justice Act 2003 and successor acts

These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

i) Equalities Act 2010

This Act aims to eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act, to advance equality of opportunity between people who share a protected characteristic and people who do not share it; and to foster good relations between people who share a protected characteristic and people who do not share it.

11. Monitoring and Reporting

The IT Department and the Leadership Team will monitor the effectiveness of this policy and will provide progress reports to the governing body.

Any monitoring will respect privacy as described above. Summary reports on Internet and E-mail use may be provided on a regular basis; managers can request more detailed analyses as described above.

The governing body will receive reports on:

- Problems encountered in implementing the policy.
- Serious breaches of the policy.
- Key issues for future development.
- A breakdown of Internet and E-mail traffic (if software allows).

However, all employees are expected to monitor their own departures from this policy statement and to ensure there is no abuse of the privilege of access to Internet and E-mail facilities.

Ack: EVH Model Policy - Communication Tools

Appendix 1

DECLARATION

All employees granted Internet and E-mail access with Association facilities will be provided with a written copy of this policy statement. All E-mail and Internet users must sign the following statement:

“I have received a written copy of my Associations E-mail and Internet usage policy statement.

I fully understand the terms of this policy and agree to abide by them.

I realise that the Associations security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file.

I acknowledge that any email message I send or receive will be recorded and stored for a finite period for management use, if required.

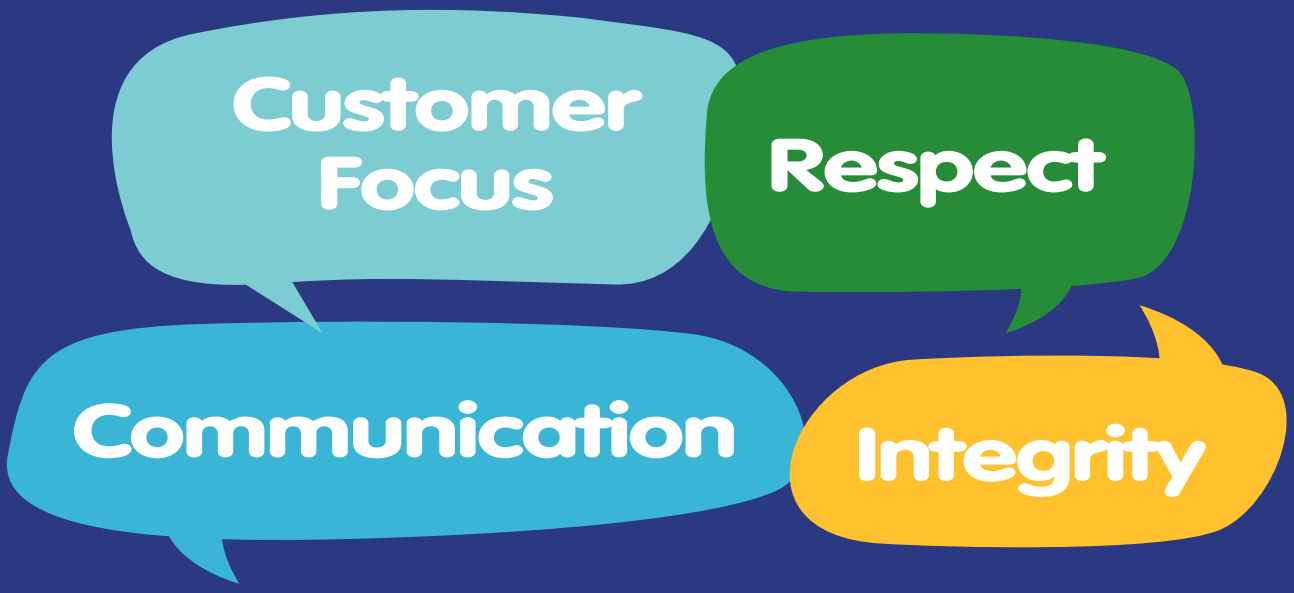
I know that any violation of this policy could lead to disciplinary action and criminal prosecution."

Signed:

Print Name:

Position:

Date:



CLOCH HOUSING ASSOCIATION LTD	
Policy Name	E-Mail & Internet Policy
Policy Category	C-HR
Policy Number	079
Date Adopted	01/04/2005
This Review	28/05/2020
Next Review	May 2023
Equalities Impact Assessment Required	No
Link to other policies	
Consultation	Yes
Need for Procedure	