Cloch Housing Association	
# ICT Acceptable Use Policy	
Policy Name	IT Acceptable Use (Replacing Email + Internet Policy)
Policy Category	C-HR
Policy Number	079
Date Adopted	01/04/2005
Last Review	28/05/2020
This Review	28/05/2023
Next Review	May 2025
Equalities Impact Assessment Required	No
Link to other policies	
Consultation	Yes

1. Definitions

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

2. Introduction

This is the Acceptable Use Policy for IT and Telecommunications equipment and services provided by the Association. It covers the use of the Associations IT network resources, client hardware (desktop PC’s, laptops, remote desktop servers, mobile phones, tablets), removal storage, Internet connections and telecommunication of all types.

All users of the Associations IT equipment and services are required to comply with this policy, and companion documents, the IT Password Policy, the Social Media Policy and the Mobile Device Agreement. Awareness of the Associations IT security approach is also essential.

Any user of the Associations IT systems whose actions violate this policy or related ICT legislation, and laws may be subject to removal of IT privileges as well as disciplinary actions.

This Policy links to Business Plan Outcomes:

Strategic Priority 14: Further develop our IT systems and software.

Strategic Priority 22: Maintain robust risk management, business continuity & disaster recovery practices.

3. Coverage

The policy covers the following elements: -

- **Client Hardware**
- **Email**
- **Internet**
- **Phone System**
- **Removeable Storage**
- **Mobile Devices**
- **Remote Access**
- **Private Messaging Applications**

This policy does not cover the proper use of passwords across the Association. This is included in the separate IT Password Policy.

This policy does not cover the proper use and administration of Social Media across the Association. This is included in the separate Social Media Policy.

4. Client Hardware

Client hardware is defined as any device that can be connected to the ICT network and used to access Association IT services. Examples of this include desktop PC's, laptops, and thin clients. Suitable client hardware is essential to allow Association staff to complete their daily tasks.

Only approved devices are permitted for use on the Associations ICT network and systems.

Any IT hardware, and data stored on it, assigned to Association staff or governing body members is the responsibility of the assigned user. The device should be used and taken care of in a secure and responsible manner.

Users of Association IT equipment should not permit unauthorised access to any devices by a third party, this includes but is not limited to, family and friends.

Policies in place prevent standard accounts installing software on Association devices. No software should be installed on a client device without IT staff authorisation.

It is recommended that no data is saved to Association devices hard drives ('C drives'). These drives are not backed up so in the event of a hardware failure, data would be lost. The Association provides both departmental and personal network storage for saving data which is backed up on a daily basis.

All Association owned client hardware has an automatic lock on idle software policy set for 10 minutes. However, for security purposes it is recommended users lock their screen should they be away from the device for any length of time.

All Association owned client hardware is held on the IT departments internal asset register which includes details such as, assigned user, warranty expiry and replacement year.

For mobile client hardware assigned to staff or governing body members, such as laptops, iPads or phones, a Mobile Device Agreement must be signed which provides greater detail and guidance on the use of those devices. (**See Section 9**)

5. Email

Email is an essential piece of technology used by Association staff and governing body members for internal and external communication. All email sent and received by the Associations email system are recorded within monitoring systems. An email filtering system is in place which scan's all incoming emails for explicit content, viruses, and SPAM.

Users of the Associations email system must always consider the security of the Associations systems and data.

The following protocols are intended to guide users on the Associations standards when using Email.

- Only those who have been authorised to use Association internet access are permitted to do so.
- Occasional personal communication via email is allowed so long as this does not interfere with staff performing their required duties.
- External email messages sent from Association accounts should have appropriate signatures and disclaimers attached.
- Users of the email system should regularly review their mailboxes and content no longer required should be discarded.
- Any users of the email system should be vigilant when opening emails with suspicious content or attachments. This also includes unexpected emails, unknown senders, known senders with unexpected email content and email with embedded links to the internet.
- If an email is suspected to have malicious content inform the IT Department.
- Care should be taken when sending emails. Users must ensure the correct recipient is selected and ensure the email address is correct before sending.
- Email must not be sent from an account a user does not have the authority to send from. This is an offence under the Computer Misuse Act.
- Association email systems should not be used to send confidential and/or personal information.

- Inappropriate email content is prohibited, this includes messages which are sexually harassing or offensive to others on the grounds of language, age, disability, race, religion, LGBTQIA+ or gender.
- Email users should not send email that could be considered defamatory criticising individuals or organisations.
- Access to another users company email account is forbidden without the explicit consent of either the account holder or account holders line manager.
- Association email should not be used to register for online services, or similar, except where there is a genuine business requirement.

6. Internet

Internet access is a key for the Association and is essential in allowing the successful operation of the Association's core business functions. The Association have systems built into the IT network to protect users and devices from malicious & inappropriate web content. The following protocols are intended to guide users on the Associations standards when using the internet and web-based resource.

- Only those who have been authorised to use CHA internet access are permitted to do so. This includes CHA staff and users of the Associations guest Wi-Fi system.
- The viewing or downloading of inappropriate material is strictly prohibited. This includes, but is not limited to, malicious software, obscene images, pornogrography, gambling, torrent downloads & piracy, religious extremist, online dating and accessing the dark web.
- Association systems should not be used to access the internet for political purposes, harassment, bullying, solicitation, or unlawful practices / acts.
- Association systems should not be used to access or promote material on the internet which brings the Association into disrepute.
- Internet file-sharing systems should not be used unless specifically allowed by the IT Department or IT Managed Service Provider.
- The Association does not recommend saving passwords or other data on internet browser applications.

Occasional personal use of Association Internet services is permitted and is covered by the same web filtering security and standards of this policy. This includes any personal device connected to guest Wi-Fi services.

All internet activity from Association devices is recorded for security purposes. This is not monitored regularly, however, the Association reserves the right to review internet usage reports for patterns and trends.

Where required, internet usage may also be monitored to assist with any internal disciplinary procedures or external requests from organisations such as law enforcement and regulatory agencies.

7. Phone System

The Association uses an internet hosted telephone system as the main communication tool for staff. This system can be installed on Association devices including (laptops, PC's, and mobile phones). It allows the phone system to be accessed from those devices and used from any location where an internet connection is available.

Staff should be aware that all external calls to/from the Association are recorded for training and monitoring purposes.

Call recording should be manually turned off when taking payments to avoid recording personal bank account information.

Out with working hours, if the Associations phone system application is installed on personal devices it must not be used for personal calls. The application should also be closed, and user extension marked as 'away'.

The Association has a separate Customer Service Standards policy which staff must follow when using Association phone systems.

8. Removeable Storage Media

Removeable storage is classed as portable hard drives connected to client hardware via USB. This type of storage is unsecure and could act as a conduit for malicious software to enter the Associations IT network.

The Association does not encourage the use of removeable storage media and should only be used in exceptional circumstances with Association issued USB pen drives.

Removeable storage media originating from outside the Association should not be inserted into Association devices under any circumstances and should be passed to IT Dept for security checks.

9. Mobile Devices

The Association utilises multiple mobile devices as part of its current IT infrastructure. Laptop's, tablets, and mobile phones are all classed as mobile devices.

The Association has a separate Mobile Device Agreement which determines the protocols staff and governing body members must follow when using mobile devices. This agreement must be completed and signed alongside the Acceptable Use Policy by any users assigned Association mobile devices for business use.

BYOD (Bring your own Device)

In some cases, the Association allows staff and governing body members to use their own devices to access Association IT resources. This includes accessing the Association's M365 portal resources and the remote access gateway.

The Mobile Device Agreement has a separate section of protocols designed specifically for BYOD and must be completed by all users who access Association IT resources on personal devices.

10. Remote Access

The Association provides the ability for users to access internal IT resources from outside the Association offices. This provides flexibility for staff and governing body members, it also facilitates contractor access to support Association software applications.

The following guidelines should be followed when accessing Association IT systems remotely.

- Two-Factor Authentication must be set up for user accounts before attempting to access Association IT systems and services remotely.
- Public Wi-Fi, which is generally unencrypted, should not be used for connecting via remote access.
- Private Wi-Fi connections used to access Association systems and services must be encrypted and require a password to establish a connection.

- Any personal device being used for remote access must have a fully security patched operating system and up-to-date endpoint antivirus.
- Devices connected remotely to Association systems should not be left unattended. Screen locks should be applied where necessary.
- The Association IT Department cannot provide technical support for external internet connection used to connect to Association IT systems remotely.
- Remote access connections must be logged out of at the end of the session. There are automatic policies in place to terminate connections after a set period of unuse.

Remote access connections may be monitored to record dates, times, and duration of access. This to provide support to users and also identify unusual usage patterns or other suspicious activity which could suggest compromised accounts or devices.

11. Private Messaging Applications

Private messaging applications have become a convenient way to connect to a group of contacts. Applications such as 'WhatsApp' are popular as they are free to use, you can converse with large numbers of people with a single message, and all messages are encrypted so there is minimal risk that messages can be intercepted by anyone outside the messaging group.

Staff should be aware that if private messaging applications are used for work purposes the following guidelines should be followed.

- Association Data Protection policies and procedures must be followed. e.g. No personal information should be shared within the group.
- All views shared by members of the group are their own and do not reflect the Associations views as a whole.
- There should be no non-Association employee members of a private group used for work purposes.
- Group messages can be used to inform colleagues of whereabouts or absences. However, the Associations official policies and procedures relating to absence and sickness must also be followed.

DECLARATION

All users of the Association IT system users must sign the following declaration:

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

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

Signed:

Print Name:

Position:

Date:
