"Offering our community more than a home"

Draft

I.T. Policy

Management Committee submission: 26 May 2020

Last Approved: 28 February 2017

Approved:

Next Review date: February 2023

Applicable CHA Objectives:

To ensure that our resources are adequate to deliver our objectives by investing in our people, demonstrating value for money and through robust procurement practices.

To provide quality, affordable housing that meets the changing needs of our customers and to ensure fair access to housing within our area.

To promote social inclusion by applying principles of equality and diversity to everything we do.

Applicable Regulatory Standards:

The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.

The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.

This document can be made available on request in a variety of different formats, such as on CD, in large print and translated into other languages.

INDEX

CLYDEBANK HOUSING ASSOCIATION LIMITED

I.T. Policy

A1. INTRODUCTION

Clydebank Housing Association (CHA) is committed to the use of Information Technology (IT) as an essential business, communication, and research tool for all staff who have access to CHA's IT facilities.

The advent of electronic mail and the Internet has greatly facilitated internal as well as external communication throughout the world. Unfortunately, this new communication tool also has the potential for misuse. It is therefore important that CHA takes adequate steps to minimise any risk to both the Association and its employees. To do so, this policy has brought together the following policies into one comprehensive IT Policy:

- E-mail and Internet Usage Policy 2011
- E-mail and Internet Usage Policy for Committee Members 2011
- Facebook Policy 2012
- Twitter Policy 2013

CHA currently has a~~n~~ contract with the IT support Company ~~contract with~~ Clearview Networks ~~which~~(a new contract will go to tender March 2021) ~~runs until 31 March 2017. Clearview~~ The IT support company provides monitoring, consultation and maintenance for all data, IT hardware and network equipment. Full details of the contract can be found in the signed service level agreement.

This policy should be read in conjunction with the Associations Data Protection Policy and Information Commissioner's (ICO) guidance, and applies to all Clydebank Housing Association commercial premises, as follows:

- Clydebank Housing Association main office, 77-83 Kilbowie Road
- Social Economy Centre, 63 Kilbowie Road
- Centre81, 2-16 Braes Avenue

A2. LEGAL FRAMEWORK

CHA aims to comply with all relevant legislation and guidance on the use of IT equipment but with the following in particular:

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Data Protection Act 2018~~1998~~
- General Data Protection Regulation 2016

- The Health and Safety at work Act 1974
- Regulation of Investigatory Powers Act 2000
- ICO Privacy and Electronic Communications Regulations

  - IT asset disposal
  - Personal information online code of practice
  - Privacy notices code of practice
  - Protecting your Personal information online
  - Social networking and online forums – when does the DPA apply
  - Bring your own device (BYOD) guidance

A3. DEFINITIONS

For the purposes of this policy the following definitions will be used:

"**IT**" for the purposes of this policy will mean any one of the following:
- Internet
- Intranet
- E-Mail
- Telephony including Mobile Devices
- Computers
- Laptops
- Fax Machines
- Smart Phones
- Tablets (e.g. iPads)
- Software

"**Electronic Data**" includes all information held electronically.
"**E-mail**" is a system of world-wide electronic communication in which a computer user can compose a message at one terminal that is generated at the recipient's terminal when he/she logs in.
"**Employees**" include all workers who are employed by the Association under a Contract of Employment, or are working for the Association as a consultant or are temporary staff or work through an agency and have access to electronic data.
"**Internet**" is a computer network consisting of a worldwide collection of computer networks that use network protocols to facilitate data transmission and exchange.
"**Intranet**" is typically an internal or restricted access network that is similar in functionality to the internet, but is only available to an organisation internally.
"**Out Of Office"** is a message automatically sent in reply to sender of an e-mail when an employee is unable to reply to the e-mail message.
"**Personal Use**" is anything not directly related to the work of the Association.
"**Social Networks**" are dedicated websites and applications to interact with other users, or to find people with similar interests to one's own.
"**Telephone Systems**" will be either landline or mobile telephony hardware used by Association staff

"**Users**" will be any employee or Committee member that uses the internet or e-mail systems via the Association's IT equipment.

"Visitors" include all external parties in our office who may require use of IT equipment, for example auditors, training co-ordinators, and in boardroom hires.

POLICY PRINCIPLES

A4. PURPOSE

This IT Policy has been produced to protect the rights of Clydebank Housing Association, its committee and staff, past, present and future, from potential threats of the Internet, the use of email, and all other IT services. This should be followed in order to help carry out the aims and objectives highlighted in the Association's IT Strategy 2016-2021. The Policy,

- Applies to all members of the Association and refers to all IT resources of the Association.
- Aims to establish basic guidelines for appropriate use of the resources.
- Details the responsibilities and obligations users have when accessing the Association's IT facilities.
- Aims to preserve confidentiality, integrity, and availability of all data.
- Forms part of all employee's terms and conditions of employment, and the rules below are contractual obligations.

A5. IMPLEMENTATION OF POLICY

- The Chief Executive Officer is responsible for the implementation and review of this policy.
- The Chief Executive Officer is responsible for ensuring Policy is up-to-date and relevant.
- The ~~Finance & IT Assistant~~DPCO Data Protection Officer and Compliance Officer (DPCO)is responsible for ensuring that all users are aware of Policy and will advise on implementation issues.
- Department Managers are responsible for ensuring all users are aware of this Policy and its application.
- All CHA employees are responsible for the security of the systems when using any CHA IT equipment in line with this Policy and must raise any potential security issues with their line manager or ~~Finance & IT Assistant~~DPCO.

Full IT implementation plan (contract with Clearview Networks) is detailed in our Disaster Recovery Procedure.

In the Absence of ~~Finance & IT Assistant~~DPCO, all related responsibilities will be covered by the Head of Housing Services ~~Housing Manager~~ (in the first instance) and the Chief Executive, who are all named custodian, responsible for the information security of each IT asset as per Data Protection Policy.

CHA will ensure that all new employees, governing body members, agency workers, contractors, and consultants will receive an induction on this policy. The policy will be integrated into all policies and procedures within CHA.

Copies of this policy will be issued to all employees, governing body members, agency workers, contractors and consultants working on CHA IT equipment and will be available to all who request it.

This policy applies to all employees, committee members, agency workers, contractors, and consultants of CHA and therefore all mentioned parties, all have a responsibility to abide by the principles outlined above and also alert their line manager or ~~Finance & IT Assistant~~DPCO should any behaviours be witnessed which breached this policy.

Unacceptable behaviour and misuse of IT equipment as described in the disciplinary section (Page 8) will not be tolerated. If a situation arises it will be dealt with immediately, as inaction is not an option. Behaviours found to be breaching this policy will be regarded as misconduct and will be dealt with appropriately and in accordance with the relevant policies, including Code of Conduct and Conditions of Service, and the Association's disciplinary procedures *may* be instigated.

POLICY

B1. NETWORK DOCUMENTATION
The Clydebank IT Network Document is a live document providing details of all network, server configuration and specifications. It ~~Includesing~~ all network service accounts\software accounts usernames and passwords. This document has restrictive access to only the DPCO and Senior Management Team.

B~~1~~2. SECURITY
Users must take appropriate measures to ensure the physical security of equipment to prevent theft, accidental damage or unauthorised access.   These include ensuring all important data is securely backed up on a network drive, users are logged off if leaving any IT device for any length of time, and all mobile IT equipment is locked away while not in use.

The Comms Room where the server is located should remain locked at all times, with only ~~Finance & IT Assistant~~DPCO, Housing Manager and Chief Executive having keys to access.

Users are not permitted to access any system or stored information unless they have been expressly authorised and enabled to do so.

All employees have access and responsibility for their own staff folder on the shared network drive and in most cases access to certain other folders throughout the network, these permissions are shown in the access mapping in Appendix 1.

All users have a duty to report all known or suspected breaches of IT security to Senior Management or ~~Finance & IT Assistant~~DPCO.

B2~~1~~.1   Passwords & Printing Authentication

Passwords
All users require a user name and password to access CHA's IT systems. To ensure their effectiveness, passwords must be as strong as possible (using a combination of numeric, letters, upper and lower case characters) and kept securely and changed regularly.

~~All users should have print settings changed to locked, so all print jobs require password authentication at the printer in order for job to be processed.~~

Users are responsible for the security of their own passwords, which protect against unauthorised access. Users should not make their password available to anyone else, nor should they use any other person's username. A password should be changed immediately if there is a suspicion that it has been compromised.

When a staff member leaves the association, their password will be changed by the ~~Finance and IT Assistant~~DPCO immediately, prior to the deletion of their profile.

Printing Authentication
All users should have print settings changed to locked, so all print jobs require password authentication at the printer in order for job to be processed.

B2~~1~~.2   Disposal
Data stored on IT equipment must be protected when the media is no longer required or do not function. All data must be physically or magnetically destroyed before media disposal. This will be performed by the ~~Finance & IT Assistant~~DPCO or by official agents on CHA's behalf. Where an external company is used to destroy the data then "certificates of secure destruction" must be obtained and stored securely for future reference. Where IT equipment is taken off site by third-party, such contractors must be bound by a confidentially agreement. If IT equipment can be re-used by others outside the Association, a secure overwriting or complete data destruction must be performed. This will be the responsibility of the ~~Finance & IT Assistant~~DPCO. All disposals are recorded in the Clydebank Asset Register.

B2~~1~~.3   Updates
~~All CHA computers have a Microsoft Windows operating system and are set to automatically deploy Windows Updates to ensure all important security fixes and settings are kept up to date. All CHA computers must also have anti-virus software installed and be configured to update automatically on a regular basis.~~

Microsoft Windows updates and anti-virus updates are centrally managed by the IT Support Company and are configured to update at a defined date and time throughout the month

All users should ensure ~~that their hard drives are defragmented every month, and~~ that computers are shut down after office hours.

If updates do not appear to be working or users experience any unusual behaviour on CHA computers, it should be reported immediately to the ~~Finance & IT Assistant~~DPCO.

B2~~1~~.4   Data Backup

Data backups of all network drives will be taken on a nightly basis and regularly tested to ensure that effective recovery can take place following any incident or operational failure. Backup tapes should be kept securely in IT safe with the previous night's version kept off-site.

Documented restoration procedures should also be stored in a remote location to avoid damage from disaster at the main site. This would act to limit data losses in the event of a breakdown or crash. Recovered data must be sufficient to provide an adequate level of service in the event of an emergency. Refer to Disaster Recovery Procedure for full details.

Restoration procedures should be checked annually to ensure they are effective and can be completed within agreed recovery time.

B2~~1~~.5   Licenses

Appropriate licenses must be obtained for all relevant programs and hardware at all times. Appropriate licenses will be checked by the DPCO and renewed by the DPCO or ~~Clearview Networks~~IT Support Company. A register of all licences will be maintained by the ~~Finance & IT Assistant~~DPCO.

B2~~1~~.6 CCTV

The use of the Association's CCTV should be done so in accordance with the principles outlined for all of CHA's IT equipment and in line with the Association's CCTV Policy. All data stored and/or passed onto appropriate and trustworthy 3rd parties such as the Police should be recorded and monitored to ensure Data Protection and CCTV Polic~~y~~ies ~~is~~are adhered to at all times.

B3~~2~~. USAGE

Users must follow the rules as set out in this policy and relevant procedures, where something is not specifically covered in this policy, employees should seek advice from their Department Manager. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the Data Protection Act 2018 ~~1998~~, Genderal Data Protection Regulations and the Association's Data Protection/Management of Information Policy.

B3.1   Internet

Use of the Internet is permitted and encouraged where appropriate but must not be detrimental to the Association's interests. Employees may access the internet for personal purposes provided access during working hours is kept to a minimum and permission sought from their line manager. Use of Internet to view, access, store, create, knowingly transmit, upload, or download inappropriate or offensive material is strictly prohibited.

It is not permissible for users to download personal software onto any CHA devices without the Chief Executive Officer/~~Finance & IT Assistant~~DPCO's consent. Users should only download files from secure websites or when they are certain that the software is virus-free.

Material on the Internet is often protected by intellectual property laws and therefore may not be copied. Users should also take care not to infringe copyright when downloading material.

CHA reserves the right to monitor users' internet usage, but will endeavour to inform users when this is to happen and the reasons for it.

B3.2   Email

The contents of e-mails should be checked carefully by users and should be treated like any other form of written communication in terms of etiquette and content, before being sent. The use of e-mail to send or forward messages which are confidential, defamatory, obscene, or otherwise inappropriate will be treated as misconduct under CHA's disciplinary procedure.

Users may send or receive e-mails for personal purposes provided it is not deemed excessive and in accordance with acceptable use. When sending personal emails, users should demonstrate the same care as when sending work-related emails.

Users should not attach any files that may contain a virus to e-mails, and should exercise extreme care when receiving attachments from third parties. E-mails should only be opened where the originator is known to the recipient. Any e-mails received with inappropriate content or attachments should be highlighted to Senior Managers immediately.

Inboxes should be maintained and all unnecessary emails deleted on an ongoing basis in order to ensure the effective running of your computer and CHA's network. Emails should be checked and cleared out quarterly.

CHA reserves the right to monitor users' e-mail usage, but will endeavour to inform users when this is to happen and the reasons for it.

Users should ensure that official corporate information is detailed on all any e-mails, with and that prior to annual leave or pre-planned absence from work, an 'out of office' reply should be added to your e-mail account. ~~An example of the email layout send with signature files and disclaimers attached is provided below:~~

B32.3   Bring Your Own Device (BYOD)

CHA does not allow employees to attach their own hardware into office IT systems without the Chief Executive Officer/Finance & IT AssistantDPCO's consent. Due to resources and expertise, CHA only offers limited technical support to personal devices being used for work purposes.

Users are not permitted to save sensitive data from CHA's network drives onto their own devices. Any device that has the Association's data on it should be secure and password protected.

Suitable antivirus software should be properly installed and running on all appropriate devices.

CHA does not accept responsibility for the loss or damage of any personal IT devices while on Association property.

CHA reserves the right not to authorise individuals, or to withdraw the authorisation, if they deem BYOD not to be appropriate and in the best interests of the Association.

B32.4   Wireless

CHA provides two wireless networks that allow access to the internet, one for staff members, the other for customers and Committee Members.users that enables access to both internet and the Associations Network drives (CHAWAP), and a separate one for

Management Committee and visitors to the office, which provides Internet access only (CHAGUEST).

Passwords to gain entry to either network will be entered onto any device by the ~~Finance & IT Assistant~~DPCO to enable automatic connection.

Devices should not be connected to an unsecure or unknown wireless network whilst being used in CHA office or while on Association business.

B32.5 Remote Use

CHA permits use of IT resources off-site where appropriate, however any equipment or software taken out of the Association's office must be signed out and in by the ~~Finance & IT Assistant~~DPCO or Senior Management.

While off-site, sensible precautions must be taken to ensure security of the Association's property at all times. In particular, you must never leave equipment on view inside a vehicle. If you have to leave such an item unattended in a vehicle, it must be locked away in the boot or glove compartment. If you are travelling on public transport or are in a public place, keep your equipment with you at all times or, if this is not possible, in sight. CHA can provide employees with remote access to their IT services in certain circumstances via the remote server desktop. This will be granted by the Chief Executive Officer or ~~Finance & IT Assistant~~DPCO for pre-arranged time slot(s), and would command all of the same rules and conduct as set out in this policy for use of CHA's IT resources.

For insurance and security purposes, lost equipment or pen drives must be reported to CHA immediately.

B2.6 iPads

~~Management Committee members are issued with iPad's in order to receive information and access their CHA mailbox. The use of these is covered by acceptable use as outlined within this policy.   All Management Committee members must read and complete iPad Terms and Conditions (Appendix 2) upon receipt of the device.~~

B2.6 Mobile Devices

Staff and Management Committee members are issued with Mobile devices including iPad's and mobile phones in order to receive information and access their CHA mailbox. The use of these is covered by acceptable use as outlined within this policy.   All staff and Management Committee members must read and sign the Mobile Device Agreement (Appendix 2) upon receipt of the device.

B3.62.7 Intranet

CHA's Intranet has been designed specifically for the use and benefit of the Association's employees and committee members as a key communication tool, to provide timely and accurate information.

A Group Policy is used to ~~CHA encourages all staff to~~ set the Intranet as their Internet "Homepage" and staff are asked to check it on a daily basis to keep up to date with Association news and documents uploaded.

C.   EQUIPMENT

All IT equipment should be purchased, used, and disposed of in accordance with the rules as set out in this policy and relevant procedures, and with the intention of fair and secure usage. All purchases and disposal are recorded in the Clydebank Asset Register

C.1   Procurement

Procurement is the acquisition of goods, services or works. It is essential that the goods/services/works supplied are appropriate for the intended purpose and, that they are procured at the best possible cost to meet the needs of the Association in terms of quality and quantity, time and location.

For the purchase of IT equipment and services, a full review will always be done to assess costs, value for money and the most appropriate procurement methods

C.2   New Purchases

New Purchases of IT equipment should be made in conjunction with information obtained from the DPCO and ~~Clearview Networks~~IT Support Company ~~and the Chief Executive.~~ Quotes and authority should be secured in accordance with Finance Procedure Note 17 and email sent to Finance and Corporate Services Manager prior to any purchase.

~~C.3   Computer Renewal Programme~~

~~All PCs should be continually monitored to ensure they can be used in accordance with CHA's IT Policy, particularly as the PCs get older and the technology they may need to use have updated. The Computer Renewal Programme and MOT Healthcheck (appendix 4 & 5) should be followed and all details kept up to date in F:\System Administration\Computer Renewal Programme Register.~~

C.3   Mobile Device and Computer Renewal Programme

The DPCO will enter all mobile devices and computer equipment into the IT Equipment Asset Register which includes information include purchase date and upgrades. In conjunction with the asset register the DPCO will monitor the condition of all mobile devices and computer equipment.

C.4   Memory Sticks

~~To ensure whilst following the PC Renewal Programme and maximising value of our assets, any data saved on any PCs is not compromised; all files that are required to be backed up should be kept in folder with relevant security permissions on the shared F:\ drive on CHAs network. All users are also given encrypted memory sticks to be used in accordance with the declaration form given for all staff to read and sign (appendix 6). If staff members require additional files to be saved, they are encouraged to save these on~~

~~their Memory Stick rather on the PCs C:\ drive to avoid them becoming inaccessible if an older machine or hard disk was to become defective while in use.~~

Memory sticks should only be utilised in very rare occasions (with express authority required from the DPCO) such as the passing of CCTV footage to the police, in these circumstances an encrypted Memory stick will be provided by the DPCO.

D. PHONE SYSTEM

The Association Telephone systems are company property, provided for use in undertaking company duties and as with other IT systems, and in accordance with current good practice and its Code of Conduct for Committee and Staff. The information created and/or stored in IT systems also belongs to the Association and can be accessed and monitored by the Chief Executive or any other senior staff at any time.

D.1 Office Phones
The Association now uses a VOIP (Voice over Internet Protocol) solution for the office landlines. This is supported alongside the IT hardware in terms of maintenance and support contract, full terms of the contract can be found in the signed service level agreement.

Any problems with the usage or hardware will now be dealt with in a timely manner using the same method as IT issues. ~~Finance & IT Assistant~~DPCO should be contacted in the first instance, who will then email relevant support helpdesk if required.

All office holiday and training closures should be covered by appropriate answer machine messages prior to the beginning of each calendar year.

D.2 Mobile Phones

The Association ensures that it has the fully inclusive mobile phone package in place for all its mobile phones which ensures that the monthly cost to the Association is fixed regardless of usage.

D.3 Personal Use
Employees are expected to use the telephone for duties they are required to undertake. However, the Association recognises that it is necessary and reasonable for employees to use the telephone for personal calls as long as they not deemed excessive and in accordance with acceptable use. Employees who have mobile telephones may have these switched on, subject to the same exceptions.

SOCIAL MEDIA

E1. Social Networking
Occasional and incidental use of social networking websites is not disallowed by CHA so long as it is not excessive and does not interfere with employees' performance of their expected duties.

CHA respects user's right to a private life and that includes joining any social media platforms users wish. However, information posted on such sites is classed as public and not private. Users are therefore not permitted to disclose confidential information and/or make derogatory or defamatory comments relating to CHA, its customers, partners, suppliers, board members, employees, stakeholders etc. on any social networking platforms. It is also prohibited to post any comments regarding people and events connected to CHA, or make any remarks which could potentially bring CHA into disrepute. Any such actions may result in disciplinary action, including dismissal.

If using social media platforms, users are expected to adhere to/note the following;
- keep profiles set to private and protect tweets.
- ensure all passwords are kept private.
- we do not prohibit employees from listing CHA as their employer however we do advise against it.
- users should be aware of the language and content of their posts – in particular where employees have an association with their employer e.g. listing their employer or linked with colleagues.

E2. Facebook
The CHA Facebook account (found by searching for Clydebank Housing Association on facebook.com) is managed by the Communications Officer, on behalf of all colleagues across the organisation. We do not use automation to post content on Facebook.

We will 'Like' organisations and people with aims and objectives broadly similar to our own or those whose posts we feel would be beneficial to our customers. 'Liking' in no way implies endorsement of any kind.

We will update and monitor our Facebook account during office hours, Monday to Friday excluding office closure as advertised on our website. Facebook may occasionally be unavailable and we accept no responsibility for lack of service due to Facebook downtime.

The purpose of the dialogue on our Facebook page is to enable as many people as possible to read and comment on our posts. We want to keep discussion as open as possible and will not attempt to exclude or edit critical opinions.
However, to protect this service from abuse, please ensure that your ideas/comments:

- are respectful of others – comments should not be malicious or offensive in nature, and should not constitute a personal attack on a person's character

- do not incite hatred on the basis of age, disability, gender reassignment, marriage, and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation or other personal characteristics
- do not include swearing, hate-speech or obscenity
- do not reveal personal details, such as private addresses, phone numbers, email addresses or other online contact details
- do not break the law – this includes libel, condoning illegal activity, and breaking copyright
- do not advertise commercial products and services. You can mention relevant products and services as long as they support your idea/comment
- are reasonably concise, and don't constitute spamming of the site
- are in English – unfortunately, we do not currently have the resource to moderate comments in other languages
- are relevant – please don't post messages unrelated to this channel or the subject under discussion
- do not breach Facebook's standard terms and conditions

Please do not impersonate or falsely claim to represent a person or organisation.

We welcome feedback and ideas from all our customers, and endeavour to join the conversation where possible.

We cannot engage on issues or answer questions which do not meet the guidelines above. We reserve the right to delete ideas and comments that breach these guidelines, and to suspend the ability to comment at any time.

We may not be able to reply individually to all the direct messages we receive via Facebook. The Communications Officer will read all direct messages and ensure that any emerging themes or helpful suggestions are passed to the relevant people within the Association.

E3. Twitter

CHA Twitter account (@clydebankha) is managed by the Communications Officer on behalf of colleagues across the organisation. We do not use any automation (such as tools which generate tweets from RSS feeds) to post content on Twitter.

We do not automatically "follow back" new followers. Being followed by us does not imply endorsement of any kind.

We will update and monitor our Twitter account during our office hours, Monday to Friday excluding office closure as detailed on our website. Twitter may occasionally be unavailable and we accept no responsibility for lack of service due to Twitter downtime.

We welcome feedback and ideas from all our followers and endeavour to join the conversation where possible. However, may not be able to reply individually to all the messages we receive via Twitter.

The Communications Officer will read all @replies and Direct Messages and ensures that any emerging themes or helpful suggestions are passed to the relevant people within the Association. We cannot engage on issues or answer questions which break the rules of our message guidelines.

Please respect other Tweeters and individuals. Tweets should not be malicious or offensive in nature and should not constitute a personal attack on a person's character:

- Do not incite hatred on the basis of age, disability, gender reassignment, marriage, and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation or other personal characteristics.
- Do not include swearing, hate-speech or obscenity.
- Do not reveal personal details, such as private addresses, phone numbers, email addresses or other online contact details.
- Do not break the law. This includes libel, condoning illegal activity, and breaking copyright.
- Do not advertise commercial products and services. You can mention relevant products and services as long as they support your comment.
- Do not impersonate or falsely claim to represent a person or organisation.
- Do not post messages that are unrelated to the Twitter feed or could constitute spamming.
- Do not post messages that breach Twitter's standard terms and conditions.

Please also note we do not currently have the resources to moderate comments in languages other than English.

TRAINING AND AWARENESS

F1. Disciplinary
Misuse of computers telephony is a serious disciplinary offence. The following are examples of misuse:

- Fraud and theft
- System sabotage
- Introduction of viruses and time bombs
- Using the system for excessive private work or any game playing
- Breaches of Data Protection Act
- Sending abusive, rude or defamatory messages
- Hacking
- Violation of the rights of any person, including rights protected by copyright, trade secret, patent, or intellectual property laws
- Breach of Organisation security procedures and IT Policy.

This list is not exhaustive. Depending on the circumstances of each case, deliberate and proven misuse of the computer system is likely to be considered a gross misconduct

offence, punishable by dismissal. Misuse amounting to criminal conduct may be reported to the police.

The Association may, from time to time, monitor employees' use of telephones, e-mail and the Internet. This will be done to:

- Assist in establishing facts which need to be known for a specific purpose
- Investigate any suspected or alleged criminal activity
- Ensure our systems work effectively (including the prevention of virus infiltration)
- Determine any suspected or alleged abuse of this policy

F2. Training
All staff or Management Committee Member responsible for using CHA's IT resources will receive the appropriate training on this Policy. It will be included, where appropriate, as part of the induction for new staff/committee (Appendix 3).

F3. Equal Opportunities
Our commitment to equal opportunities and fairness will apply irrespective of factors such as race, sex, disability, age, gender reassignment, marriage & civil partnership, pregnancy & maternity, religion or belief and sexual orientation.

F4. Declaration Form
I have read and understood this IT Policy and hereby accept the rules therein as being binding upon my Terms and Conditions of Employment/Management Committee Code of Conduct with the Association. I understand that failure to adhere to the Policy may result in disciplinary action or my dismissal from the Association.

Signature:	
Date:	
Name:	
Location:	

For Office Use Only – Actions

Customer Consultation Required/Arranged	No
Intranet Update	Yes
F Drive Update	Yes
Website Update	Yes
Leaflet change required?	No
Newsletter Promotion?	No
Other information updated, e.g. posters, automatic email responses, post cards, answering machine messages, etc.	No
Equality Impact Assessment completed	Yes

Appendix 1 - New Staff I.T Induction

•   Register user - Username: _____ / Password: _____

•   Installing software on profile
o   Sage – Logon: _____
o   Kypera – Username:_____ / Password:_____

•   Email
o   Email address – _____@clydebank-ha.org.uk

•   Printing – Default printer: _____

•   Saving to a network drive
o   F drive (network drive) – Staff Folders/_____

•   Security
o   Setting and recovering your password

•   How to log a problem with Systems Admin

•   IT Policy

Appendix 12 – Network Drive Access Mapping

Clydebank Housing Association 17/02/2017		Shared Network Drive - Access and Permissions Matrix	
Folder	Address	Authorised Staff	Permissions
A- Documents in Different	F:\A- Documents in Different	SK/LL/JF/AMacF/Ali/SB	Read write Modify
Formats List	Formats List	All Staff	Read only
ALLPAYCONNECT	F:\ALLPAYCONNECT	SK/LL	Read write Modify
		All Finance Staff/MMcK	Read write
		All Staff	Read only
APSR	F:\APSR	SK	Read write Modify
		LL/JF/AMcF	Read write
		All Staff	Read only
Carduus	F:\Carduus	SK/LL/JF/AMacF	Read write Modify
		All Staff	Read only
Centre81	F:\Centre81	SK/Ali/LL	Read write Modify
CHA Power	F:\CHA Power	SK/HMcL/LL	Read write Modify

		Finance Staff/AMacF	Read write
		All Staff	Read only
Communications	F:\Communications	SK/LL/JF/AMacF/Ali/SB	Read write Modify
		All Staff	Read only
Complaints and	F:\Complaints and Compliments	All Staff	Read write Modify
Compliments			
Consultation Register	F:\Consultation Register	SK/SB/Ali	Read write Modify
		LL/JF/AMacF/	Read write
		All Staff	Read only
Development Opportunities	F:\Development Opportunities	SK	Read write Modify
		LL/JF/AMacF/	Read only
Estate Management	F:\Estate Management	SK/ HM staff/ Maint Staff	Read write Modify
		All Staff	Read only
Factoring Folder	F:\Factoring Folder	SK/LL/FCW/AMacF/MMcL	Read write Modify
		All Staff	Read only
Factoring Folder	F:\Factoring Folder	All Staff	Read write Modify
	\Factoring Call record		
Finance & Admin Folder	F:\Finance & Admin	SK/LL/FCW Only	Read write Modify
	\Salary & Pension details		
Finance & Admin Folder	F:\Finance & Admin	SK/LL/FCW/MMcL	Read write Modify
		All Staff	Read only
Finance & Admin Folder	F:\Finance & Admin\	SK/LL/FCW/MMcL Only	Read write Modify
	Bank Reconciliations		
Finance & Admin General	F:\Finance & Admin General	SK/All Finance Staff	Read write Modify
		All Staff	Read only
Finance & Admin General	F:\Finance & Admin General\Credit	SK/SB/All Finance Staff	Read write Modify
	Card Expenditure	All Staff	Read only
General Folder	F:\General Folder	SK/LL/JF/AMacF	Read write Modify
		All Staff	Read write
Housing Management	F:\Housing Management Folder	SK/JF	Read write Modify
Folder		All Housing Mgt Staff	Read write
		All Staff	Read only
Housing Management	F:\Housing Management Folder\	SK/JF	Read write Modify
Folder	Allocations and voids	All Housing Mgt Staff/SB	Read write
		All Staff	Read only
Housing Management	F:\Housing Management	SK/JF	Read write

			Modify
Folder	Mg\Inspections	All Housing Mgt Staff/SB	Read write
		All Staff	Read only
Housing Management	F:\Housing Management Folder\ Rents	SK/JF	Read write Modify
Folder	\Housing Benefit	All Housing Mgt Staff/Janet	Read write
		All Staff	Read only
Internal Audit March 2015	F:\Internal Audit March 2015	SK/LL/JF/AMacF	Read write Modify
		All Staff	Read only
Kypera Housing	F:\Kypera Housing	SK/JF/AMacF	Read write Modify
		All HM /All Maint Staff	Read write
		All Staff	Read only
Maintenance Folder	F:\Maintenance Folder	SK/AMacF	Read write Modify
		All Maintenance Staff	Read write
		All Staff	Read only
Maintenance Folder	F\Maintenance Folder\Major	SK/AMacF/SB	Read write Modify
	Repairs\Controlled Entry Upgrade	All Maintenance Staff	Read write
	– Band 1 Core Stock	All Staff	Read only
Maintenance Folder	F\Maintenance Folder\Tenant	SK/AMacF/SB	Read write Modify
	Satisfaction Surveys	All Maintenance Staff	Read write
		All Staff	Read only
Management Committee	F:\Management Committee	SK/JF/AMacF/LL	Read write Modify
		All Staff	Read write
MMR	F:\MMR	SK	Read write Modify
		LL/JF/AMacF	Read write
		All Staff	Read only
OFT	F:\OFT	SK/LL	Read write Modify
		All Staff	Read only
Policy & Procedure Folder	F:\Policy & Procedure Folder	SK/JF/AMacF/LL	Read write Modify
		SB/FCW/MMcL/CB/SS/GS/SJ	Read write
		All Staff	Read only
Reception Admin Folder	F:\Reception Admin Folder	SK/LL/AMcD/SB/JF	Read write Modify
		Finance Staff	Read write
		All Staff	Read only
Scottish Social	F:\Scottish Social Housing Charter	SK	Read write Modify
Housing Charter		LL/JF/AMacF/SB	Read write
		All Staff	Read only
Shared Equity Information	F:\Shared Equity Information	SK	Read write Modify
		All Staff	Read only

Staff Absence Information	F:\Staff Absence Information	SK	Read write Modify
Staff Folders	-F:\Staff Folders	AMacF/JF/LL/Ali SK Secondary Admin Staff Folders RO Staff Folders MOD User Data Access Group	Read only Modify Modify Read Modify List
Staff Member Folders	F:\Staff Folders\Staff Name	All StaffSK Staff Member	Read only Modify Modify
Alan Thompson	F:\Staff Folders\Alan Thompson	SK/AT	Read write Modify
-	-	All Staff	Read only
Alison Macfarlane	F:\Staff Folders\Alison Macfarlane	SK/AMacF	Read write Modify
-	-	All Staff	Read only
Alison Mailey	F:\Staff Folders\Alison Mailey	SK/Ali	Read write Modify
		All Staff	Read only
Archived Staff Folder	F:\Staff Folders\Archived Staff Folders	SK	Read write Modify
		AMacF/JF/LL	Read write
		All Staff	Read only
Catherine Banks	F:\Staff Folders\Catherine Banks	SK/AMacF	Read write Modify
-	-	All Staff	Read only
Chato Mashimango	F:\Staff Folders\Chato Mashimango	SK/CM	Read write Modify
-	-	All Staff	Read only
Debbie Brown	F:\Staff Folders\Debbie Brown	SK/DB	Read write Modify
-	-	All Staff	Read only
Drew McDougall	F:\Staff Folders\Drew McDougall	SK/AMcD	Read write Modify
-	-	All Staff	Read only
Fiona Campbell	F:\Staff Folders\Fiona Campbell	SK/FC	Read write Modify
-	-	All Staff	Read only
Fiona White	F:\Staff Folders\Fiona White	SK/FCW	Read write Modify
-	-	All Staff	Read only
George Stevenson	F:\Staff Folders\George Stevenson	SK/GS	Read write Modify
-	-	All Staff	Read only

~~Jack Devlin~~	~~F:\Staff Folders\Jack Devlin~~	~~SK/JPD~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Janet Dunphy~~	~~F:\Staff Folders\Janet Dunphy~~	~~SK/JD~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Joan Craig~~	~~F:\Staff Folders\Joan Craig~~	~~SK/JC~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Joe Farrell~~	~~F:\Staff Folders\Joe Farrell~~	~~SK/JF~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Lynette Lees~~	~~F:\Staff Folders\Lynette Lees~~	~~SK/LL~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Margaret McKeitch~~	~~F:\Staff Folders\Margaret McKeitch~~	~~SK/MMcK~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Michael McLaughlin~~	~~F:\Staff Folders\Michael McLaughlin~~	~~SK/MMcL~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Rae Carruthers~~	~~F:\Staff Folders\Rae Carruthers~~	~~SK/RC~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Sam Joyce~~	~~F:\Staff Folders\Sam Joyce~~	~~SK/SJ~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Sharon Keenan~~	~~F:\Staff Folders\Sharon Keenan~~	~~SK/SK~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Sinead Boyle~~	~~F:\Staff Folders\Sinead Boyle~~	~~SK/SB~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
~~Stacy Shaw~~	~~F:\Staff Folders\Stacy Shaw~~	~~SK/SS~~	~~Read write Modify~~
~~-~~	~~-~~	~~All Staff~~	~~Read only~~
Staff Information	F:\Staff Information	SK	Read write Modify
		LL/JF/AMacF/SB	Read write
		All Staff	Read only
Stock Transfer	F:\Stock Transfer	SK	Read write Modify
		All Staff	Read only
System Administration	F:\System Administration	SK/MMcL	Read write Modify
		JF	Read write
Training Library	F:\Training Library	SK/	Read write Modify
		LL/JF/AMacF/SB	Read write
		All Staff	Read only
Value for Money Folder	F:\Value for Money	SK/AMacF/JF/LL/MMcL	Read write Modify

			All Staff	Read only
Void Management Folder	F:\Void Management Folder	SK/AMacF/JF	Read write Modify
		All HM /All Maint Staff	Read write
		All Staff	Read only
Wider Role	F:\Wider Role	SK/Ali/SB	Read write Modify
		LL/JF/AMacF/	Read write
		All Staff	Read only

iPad Terms and Conditions

I have received CHA Apple iPad No. _____ and cover in brand new condition. I understand that the iPad and cover remains the property of Clydebank Housing Association Ltd (the 'Association'). I agree as follows:

- that the iPad and all software, applications (apps) and accessories supplied with it are owned by and/or licensed to the Association

- to comply with any licence terms in respect of software or apps supplied with the iPad

- that I will only download free software and apps

- that I am responsible for any software and apps I load onto the iPad and that I will comply with any licence terms in respect of the software and apps

- to take all possible precautions with regards to the safety, security and general care of the iPad

- to ensure a password is used to protect the iPad at all times

- not to allow any unauthorised third party to use or otherwise access the iPad

- to report a theft of the iPad immediately to the police and CHA and obtain an incident number. I understand I must pass the incident number to the Association as soon as practically possible for insurance purposes

- to report any damage to the iPad, accidental or otherwise, to the Association's office as soon as is practically possible

- to adhere to the Association's Internet and E-mail Usage Policy for Committee Members and to comply with all requests made by the Association in connection with use of the iPad

Continued overleaf

- to return the iPad immediately or make it immediately available for collection if requested by the Association

- to make the iPad available for maintenance (such as Apple or system upgrades) as and when requested by the Association

- to bring the iPad to all committee meetings

- to undertake appropriate training provided by the Association

- to inform the Association if there is any reduction or increase in the cost of any broadband internet connection in respect of the cost the Association is reimbursing me

- to return the iPad and any accessories supplied with it to the Association immediately on leaving the Management Committee

Name:

Address:

Sign: _____

Date: _____

Appendix 3 Staff Mobile Device Agreement

clydebank housing association

Mobile Device Terms and Conditions

I have received the following mobile device(s) and accessories.

Item	Device Name	Description	Serial Number	IMEI Number	Tel No.
iPhone	CHA-MO-X	iPhone 7 32GB	DX3ZDLXXXX	356388102XXXXXX	079318439999
iPhone Charger					

I understand that the mobile device(s) and accessories remains the property of Clydebank Housing Association Ltd (the 'Association'). I agree as follows:

- that the Mobile device(s) and all software, applications (apps) and accessories supplied with it are owned by and/or licensed to the Association

- to comply with any licence terms in respect of software or apps supplied with the Mobile device(s)

- that I will only download free software and apps

- that I am responsible for any software and apps I load onto the Mobile device(s) and that I will comply with any licence terms in respect of the software and apps

- to take all possible precautions with regards to the safety, security and general care of the Mobile device(s)

- to ensure a password is used to protect the Mobile device(s) at all times

Mobile device(s) Receipt Continued

- not to allow any unauthorised third party to use or otherwise access the Mobile device(s)

- to report a theft of the Mobile device(s) immediately to the police and CHA and obtain an incident number. I understand I must pass the incident number to the Association as soon as practically possible for insurance purposes

- to report any damage to the Mobile device(s), accidental or otherwise, to the Association's office as soon as is practically possible

- to adhere to the Association's Internet and E-mail Usage Policy for Committee Members and to comply with all requests made by the Association in connection with use of the Mobile device(s)

- to return the Mobile device(s) immediately or make it immediately available for collection if requested by the Association

- to make the Mobile device(s) available for maintenance (such as Apple or system upgrades) as and when requested by the Association

- to undertake appropriate training provided by the Association

- before leaving the Association to return the mobile device(s) and any accessories supplied.

Name:

Position:

Sign: _____

Date: _____

REMOVE All BELOW HERE

Appendix 3 – New Staff I.T Induction

Clydebank Housing Association   IT Induction

- Register user – Username: _____ / Password: _____

- Installing software on profile
  - Sage – Logon: _____
  - Kypera – Username: _____ / Password: _____

- Email
  - Email address – _____@clydebank-ha.org.uk

- Printing – Default printer: _____

- Saving to a network drive
  - F drive (network drive) – Staff Folders/_____

- Security
  - Setting and recovering your password

- How to log a problem with Systems Admin

- IT Policy

Signed (Employee): _____   Date: _____
Signed (Finance & IT Assistant): _____   Date: _____

Appendix 4 – Computer Renewal Programme

INTRODUCTION
Computers play a vitally important role for Clydebank Housing Association to provide the services required by our customers. In our main office we have 21 users all with desktop computers that are operated as an integral part of each user's jobs. We also have computers offsite, used by both our caretakers and Centre81 staff, and laptops available for temporary use for members of staff or guests to our office.

Aged and degrading computer hardware is a major source of reduced productivity and staff time, not to mention frustration and dissatisfaction, within any office. To prevent these negative consequences it is important to keep records of all equipment; including the date purchased, length of warranty, and to frequently monitor and test equipment in order to maintain hardware.

Employing a Computer Renewal Programme would assist the Association in ensuring all monitoring is carried out easily and the efficiency of all hardware remains uncompromised with updates, upgrades or replacements done in as timely and economic manner as possible.

PRINCIPLES
The average lifespan of a desktop computer is 4 years and can often be referred to as obsolete after 5 years. The longevity of hardware can often depend on what it is used on a daily basis, and what changes and updates in software there have been in that period. Capital purchases such as computers are depreciated over 3 years, so effectively are no longer of financial value to the Association. The standard recommendation is to replace hardware after 3-4 years, however if managed closely and still performing adequately, it is important for the Association to get the greatest value out of all hardware purchased.

In order to get the most of the financial spend on our computers, the Computer Renewal Programme outlined in this document will be carried out.

Computers can begin to fail in varying ways, and it can often be difficult to diagnose whether there is an individual stand-alone issue which can be fixed, or if it related to a more comprehensive decline in the hardware which would require a more serious upgrade or replacement.

In order to assess whether replacement would be necessary; it is important to take into consideration the age of the hardware, the costs that would be involved in repairing or upgrading, and the likelihood of recurring or consequent problems caused by doing so.

Renewal is generally recommended when the overall cost of upgraded parts is more than 50% of the cost of a newer and better system; however each situation should be taken on its own merit after monitoring the hardware and gathering quotes for upgrades and

replacements.   The use of a cost-effective replacement programme helps balance the cost, the usefulness, and the efficiency of how CHA as an organisation manage and use our IT assets.

IMPLEMENTATION
All CHA computer users should be operating all IT equipment in accordance with the Association's IT Policy in order to maintain all hardware and software effectively, and inform the Systems Administrator if there are any error messages or noticeably underperforming programs.

It is the responsibility of the Systems Administrator to monitor all items on the Computer Renewal Programme register, carry out the relevant checks when appropriate, and to provide recommendations for any of failing hardware used by CHA users.

Clearview Networks will be consulted on all purchases of new hardware to be used on the Associations network, and the Chief Executive will be required to approve all purchases over £500.

COMPUTER RENEWAL PROGRAMME
Regardless of whether problems have been previously highlighted or not, 5 years after their initial purchase, each computer will be assessed.

All machines will receive the same PC MOT Health Check (appendix 1) to consider its suitability for continued use or further action.

A pre-inspection should be carried out by computer user to highlights any initial issues and procedures which could be carried out prior to the Systems Administrator's Health Check inspection.

The main inspection should establish if any of the following resolutions should be made:-

- Computer is over 5 years old and has 3 or more issues highlighted in the exterior, interior, or performance checks that cannot be fixed through problem solving alone. Unless Clearview Network indicates a sustainable upgrade could be carried out significantly cheaper, a recommendation that a renewal would be required.
- Computer is less than 5 years old and 5 issues highlighted, a similar approach to above would be recommended (obviously replaced via warranty if within applicable timeframe).
- Computer is less than 5 years old but underperforming with fewer than 5 issues on the inspection highlighted, we would advocate managing the machine within the association if this could be done without a significant loss of time or productivity. In such situations, switching machines for other alternatives within the Association where users may require lesser functionality or older software are worth pursuing.

After inspection and any consequent scans, changes, or updates to software – Recommendations should be made on the Health Check, and consultation made with Clearview Network and Chief Executive.

A Computer Renewal Programme Register is kept in F:/System Administration containing all up to date information for reference along with all scanned Health Check form.

Appendix 5 – PC MOT Health Check

PC MOT Health Check		

User Details   Date ☐

Name ☐

Dept. ☐	Job Title ☐
PC ☐	Serial No ☐
Make ☐	Model ☐	Purchased ☐

Previous Modifications/Upgrades

---

clydebank
clydebank housing association

77-83 Kilbowie Road | Clydebank G81 1BL
0141 941 1044 | www.clydebank-ha.org.uk

Pre-Inspection

Running well (not noticeably slowly)	☐
Not Crashed (or produced error messages) more than once in past week	☐
No MacAfee or Windows updates overdue	☐
Running latest version of Windows (or other operating system)	☐
Successfully runs all programs necessary to carry out users job	☐
Connect to any shared drive/device/Other hardware	☐
Defrag carried out in last 4 weeks	☐
User is Happy with PC	☐

Inspection				**Post-Inspection**	
Details		Y	N		
Computer less than 5 years old		☐	☐	C:/ files saved to memory stick	☐
First PC MOT carried out on this machine		☐	☐	Physically cleaned	☐
PC has had no major previous performance issues		☐	☐	Reset auto updates	☐
Exterior				Run Malware Scan	☐
No visual Damage		☐	☐	Run Sytem Restore	☐
No Excessive noise when in use		☐	☐	Uninstall programs	☐
PC Temperature normal (not phyically warm)		☐	☐	Re-install windows	☐
Interior					
Has at least 4 GB of RAM		☐	☐		
Hard drive has at least 25% space free		☐	☐	**Recommendations / Comments**	
Has adequate slots for current devices/hardware		☐	☐		
Performance					
Takes less than 5 minutes to start up		☐	☐		
Closes down successfully in less than 5 minutes		☐	☐		
Restarts successfully		☐	☐		
Runs 4 Apps concurrently without crashing		☐	☐		
System restore point available from past week		☐	☐		
All drives automatically connect/map at start up		☐	☐		
Reads and saves files from memory stick		☐	☐		
Opens browser in less than 1 minute		☐	☐		

Signed ☐   Date ☐

Clydebank Housing Association Ltd   **Encrypted USB Memory Stick**

Declaration Form

I have received 16GB USB Memory Stick in brand new condition. I understand that this remains the property of Clydebank Housing Association Ltd (the 'Association'). I agree as follows:

- As with all CHA IT equipment and data, this will be used in accordance with terms and conditions set out in the Association's IT Policy.

- To use the Memory Stick for any files you wish to save outwith the Shared F:/ drive, and replaces any requirement to save on your computers C:/ drive.

- Files found on C:/ drive during any routine check or maintenance of your computer will be moved to your memory stick.

- There should no longer be files kept on your computer's desktop, with only shortcuts to documents or icons for software programmes located there.

- To ensure a secure password is used and not shared with anyone else.

- Not to allow any unauthorised third party to use or otherwise access the Memory stick.

- To report any damage, loss, or theft to the Systems Administrator as soon as practically possible.

- To bring the memory stick to work for use each day.

Signature:	
Date Received:	
Name:	