CLYDESDALE HOUSING ASSOCIATION LIMITED

Policy:	Information Communication Technology Code of Practice
Date:	26 June 2019
Lead Officer:	Chief Executive
Review Date:	June 2022
Regulatory Standard:	**Standard 4** The governing body bases its decisions on good quality information and advice and identifies and mitigates risk to the organisation's purpose.
Regulatory Guidance:	4.3 The governing body identifies risks that might prevent it from achieving the RSL's purpose and has effective strategies and systems for risk management and mitigation, internal control and audit.
Regulatory Standard:	**Standard 5** The RSL conducts its affairs with honesty and integrity.
Regulatory Guidance:	5.1 The RSL conducts its affairs with honesty and integrity and, through the actions of the governing body and staff, upholds the good reputation of the RSL and the sector. 5.2 The RSL upholds and promotes the standards of behaviour and conduct it expects of governing body members and staff through an appropriate code of conduct. It manages governing body members' performance, ensures compliance and has a robust system to deal with any breach of the code.

Clydesdale Housing Association will provide this policy on request at no cost, in large print, in Braille, in audio or other non-written format, and in a variety of languages.

HAPPY TO TRANSLATE

1 INTRODUCTION

1.1 Clydesdale Housing Association (CHA) recognises the essential role Information Communication Technology[1] (ICT) plays in the conduct of its business and values the significant benefits and efficiencies achieved in communication with colleagues, residents, stakeholders and other business contacts. This Code of Practice, including Appendix 1, sets out the guidelines and responsibilities that support the use of ICT. It aims to clarify what is good practice when using electronic equipment, static or removable and what is unacceptable practice.

1.2 How an employee communicates with customers not only reflects on them as an individual but on CHA as an organisation: its reputation, good practice and statutory compliance. While respecting personal autonomy and privacy, these guidelines provide best practice to protect individuals, their data, CHA information and other assets.

1.3 CHA will review the ICT Strategy, ICT Code of Practice and any associated procedures regularly considering equal opportunity implications and taking appropriate action to address inequalities likely to result or resulting from their implementation.

1.4 This Code may be changed without notice for a variety of reasons; if this happens details of the change(s) will be issued in writing. Individuals will be asked to confirm acceptance of the change(s).

2 COMPLIANCE

2.1 All employees must comply with this Code at all times and must inform their manager if they feel that they are, or may be, unable to do so for any reason. By using CHA's ICT equipment you will be deemed to have agreed to the terms set out in the Code.

2.2 The Corporate Services Officer (CSO) is responsible for ensuring that all new staff, understand, sign and retain a copy of this Code of Practice within 7 days of commencing employment. Managers must take steps to ensure that team members conform with and follow the Code. The original signed declaration must be returned to the CSO for filing in their personnel file.

2.3 The Code does not intend to be restrictive or impinge on personal rights or privacy, however, the processes and controls described must be vigorously adhered to. It is important that each section is read carefully, as individuals will, for the duration of their employment, be deemed to be aware of its contents in the event that there is any breach of the Policy. **Always ask before acting.**

2.4 Any inappropriate use of CHA's ICT systems, whether under this Code or otherwise, may lead to disciplinary action being taken against the individual under CHA's disciplinary procedures which may include summary dismissal

3 CODE OF PRACTICE

3.1 Infrastructure/Software

3.1.1 New employees will be given a personal login to access the CHA system and a CHA email address. All staff will have access rights to Microsoft Office: Word, Excel, PowerPoint, Outlook and access rights to the system, including SDM software as appropriate to their role. Please refer to practice directives: Appendix 1.

[1] PCs, email, internet, phone, fax, mobile devices (laptops, tablet, mobile phone), removable media, multi-function devices e.g. printer/scanner/fax.

3.1.2 Access to folders within the CHA Novell drive will be restricted to folders containing relevant resources to individual staff member roles. Staff members requiring access to restricted resources must make a request to their line manager – the CEO will make final decisions on access rights based on system security and practical considerations.

3.2 Email

3.2.1 All emails sent or received through CHA's exchange are part of official CHA records. CHA can be legally compelled to show that information to law enforcement agencies or other parties[2]. Please refer to practice directives: Appendix 1.

3.2.2 CHA ICT systems are provided for legitimate business purposes. While respecting the privacy of individuals, CHA reserves the right to monitor employee use of email and, in certain circumstances, if deemed necessary to access and record staff communications for business purposes which include the following:

1. providing evidence of business transactions;
2. ensuring business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of CHA's communications systems or criminal activities;
5. maintaining the effective operation of CHA's communication systems;
6. ensuring continuity of service e.g. period(s) of staff absence.

Any such examinations or monitoring must be instructed by a member of the Management Team.

3.2.3 CHA respects and operates within copyright laws. Users may not use corporate email to share any copyrighted software, media or materials owned by third parties, unless permitted by that third party. Individual business email accounts will be in the CHA corporate standard with corporate email signature including the corporate disclaimer. This must not be removed or changed.

3.2.4 Employees must not use the corporate email system to perform any tasks that may involve breach of copyright law. Users should be aware that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright.

3.2.5 Staff are permitted to use corporate email account for personal use, subject to the following:

1. Personal email use must be of a reasonable level and restricted to personal time and must not be sent during work time;
2. Personal email use must not affect the email service available to other users. For instance, sending files greater than 10MB by email will slow or cease service.

3.2.6 Staff **are not** permitted to access their own personal email accounts using the CHA network. CHA email systems are secured against viruses and other malware, however, the same security cannot be extended to e-communications via personal email providers.

3.3 Internet

3.3.1 CHA acknowledges the efficiency benefits of using the internet to achieve corporate and team objectives. The internet must be used responsibly and professionally. Viewing or distributing inappropriate content is a breach of the Code of Conduct and is not acceptable under any circumstances. Employees **must not** use any corporate systems or equipment to**:**

[2] Not limited to but may include Subject Access Requests, internal investigations, FOI requests.

1. View, download, create or distribute any inappropriate content[3] or material, engage in any activities that are illegal or criminal or could adversely affect CHA's reputation;
2. Create or transmit material that might be defamatory, offensive, harassing or incur liability for CHA;
3. Broadcast unsolicited personal views on social, political, religious or other non-business related matters;
4. Introduce any form of computer viruses or carry out other hacking activities.

3.3.2 Public Wi-Fi is available as a service to CHA customers. Staff are permitted to access the public Wi-Fi___33 on personal devices. As a security measure, the password will be changed weekly.

3.3.3 CHA employees may use the corporate internet system for personal reasons, subject to the following:

1. Personal internet use should be of a reasonable level and restricted to personal time and is not permitted during work time.
2. The Code of Practice for business use, applies equally to personal internet use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.
3. Personal internet use does not impact on the internet service available to staff for business use. For instance, downloading large files or streaming music / videos may slow access for other employees.

3.3.4 The internet can, sometimes inadvertently be a source of significant risk and security exposure with the potential to cause significant damage to CHA's data, systems and reputation. CHA will use web filtering software to reduce the risk of attack, however, users must always consider the security of CHA's systems and data when using the internet and must not knowingly introduce any form of computer virus, Trojan, spyware or any other malware into CHA's network. Password's should be strong and changed regularly. Internet usage reports will be produced regularly and monitored.

3.4 **Social Media Platforms**

3.4.1 CHA respects the right to a private life and that includes joining any social media platforms employees wish. However, information posted on such sites is classed as public and not private. Employees are therefore not allowed to disclose confidential information relating to CHA, its customers, partners, suppliers, committee members, employees, or stakeholders on any social networking platforms. It is also prohibited to post any comments on people and events connected to CHA, or make any remarks which could potentially bring CHA into disrepute. Any such actions could result in disciplinary action, including dismissal.

3.4.2 If using social media platforms employees are expected to adhere to the following:

1. Keep profiles set to private and protect tweets.
2. Ensure all passwords are kept private.
3. We do not prohibit employees from listing CHA as their employer, however, we do advise against it.
4. Avoid personal social media connections with CHA's service users, suppliers and stakeholders.
5. Employees 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.

[3] text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by law

3.5 Portable Media/Removable Devices

3.5.1 Removable Media and Portable Devices[4] can be described as easily portable items used for mobile computing through connection to or by removal from another computing device or on its own. Staff must employ good practice and take all reasonable measures to prevent loss, damage or theft. Please refer to practice directives: Appendix 1.

3.5.2 CHA staff may only use CHA removable media with CHA computers/electronic devices. CHA removable media may not be connected to or used in computers that are not owned or leased by CHA without explicit permission of the CSO. Personal devices may be connected to computers for charging purposes only.

3.5.3 Sensitive information should be stored on approved removable media only as necessary for staff carrying out duties or when providing information to other approved 3rd party agencies.

3.5.4 Sensitive information stored on removable media should be encrypted prior to removal from CHA premises. All removable media & portable devices will be controlled by the CSO and recorded in the Asset Register to ensure adequate monitoring of CHA's data.

3.5.5 Any portable devices used by staff and which store sensitive content must have encryption enabled. Sensitive corporate and personal identifiable information must not be stored or transferred using any unencrypted "USB Memory" device. Information must not be stored permanently on portable devices. Information must be deleted or saved to an appropriate location at the earliest opportunity. Applications for Encrypted Memory devices should be made to the CSO.

3.5.6 If a member of staff is given a device in order for them to be contactable then their mobile device should be on at all times during business or 'on-call' hours, except when driving or when the user deems it inappropriate due to work reasons for example when in a meeting.

3.5.7 For user's protection all portable devices have location software enabled, this **must not** under any circumstances be disabled.

3.5.8 Any non CHA removable media must be scanned for viruses & other malware prior to business use, e.g. memory sticks from external trainers. Please seek advice from the CSO.

3.5.9 Access to CHA network for any external visitors or 3rd parties should be via the 'CHA Public' wireless network only. Under no circumstances should any non-CHA device be allowed access to the CHA network with the use of a network cable.

3.5.10 When taking digital images or audio recordings using portable devices it is important to consider your responsibilities regarding privacy; the security of the image; professional responsibilities and legal obligations and ensuring that where appropriate that the image becomes part of the customer's record to allow auditability of digital images or audio recordings taken.

3.5.11 All public sector organisations are now directed to ensure all digital information that is either person identifiable or otherwise sensitive, is encrypted to appropriate standards. This mandate applies to both the storage of, and transfer of any such digitally held information. If you are concerned or unsure how to secure digital images or audio recordings in this way, please contact the CSO for further advice

[4] include laptops, desktops, tablets, mobile phones, digital cameras, and portable/external hard drives, CD's, DVD's USB Memory Sticks (Pen/flash drives) and SD Cards

4 DECLARATION

I …….confirm I have read and understood the terms of this Code of Practice and I agree to uphold its requirements in all my activities as a staff member of Clydesdale Housing Association.

I understand that if I am found to have breached any points mentioned in this Code of Practice or acted against its spirit, action will be taken in accordance disciplinary procedures and could ultimately result in my dismissal.

Signed ……

Date ……

Appendix I – Practice Directives

INFRASTRUCTURE/SOFTWARE	
DO's	**DON'T's**
Change system password every month. Close files when finished working on them to allow colleagues access and log out of the system when leaving the room. Close down PC completely at least every week, but preferably at the end of the working day.	Divulging password to another person. Going to lunch/meeting without closing files and logging out or locking PC. Not closing down at end of working day.
EMAIL	
Use appropriate behaviours and formal business language when communicating by email. This applies to emailing on company premises or remotely, using CHA equipment or personal equipment. Consider if email is genuine, could it be spam that may be harmful? – were you expecting email? /does the language and content appear to be unusual? If in doubt, do not open and forward to SABRE SYSTEMS. If sending sensitive data to external email e.g. list of tenant's phone numbers, account balances, etc., then ensure documents are password protected. Document and password should be sent in separate emails - never together. Ensure the subject line is meaningful and reflects content. Apply 'High Importance' sparingly and only where a message is genuinely a priority. Avoid requesting a 'message read' receipt as not all email services support them. Be sparing with group messages; consider who needs to be added as 'CC' and only use where the recipient may be impacted by the contents of the email. Consider 'Reply All', do all colleagues require to be involved? Valuable resources are used every time an email is delivered to an inbox. Use the 'BCC' (blind carbon copy) field to send group messages where appropriate. It stops an email recipient seeing who else was on the email. Can be used to protect from the distribution of personal email addresses. Use hyperlink instead of attaching a file to an internal email to avoid numerous versions of files and to ensure all colleagues work with the same document.	Using, creating or distributing inappropriate language, content[5] or material, received or sent by email; breach of Code of Conduct. Opening attachments from unknown senders without checking if it's genuine. Forwarding chain emails or 'humorous' messages. These have the potential to detract from work related material and cause offence. Using email for criminal activity. Sending unprotected personal information by email. Don't leave subject line blank or use words like 'Hi'. Never use all capital letters in messages or subject lines. This can be perceived as impolite or shouting. Files greater than 10MB should not be sent via email, this could 'block' the mail exchange as the file size is considered excessive. Enquire with Corporate Services Officer for alternative solutions. Including large amounts of info that will need accessed at a later date within the body of an email.

[5] text, images or other media that could reasonably offend someone on the basis of race, age, gender, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by law

Users should ensure regular upkeep of inbox, sent items and deleted items. Systems should be employed for safe and appropriate storage of important emails.	

SOCIAL MEDIA PLATFORMS	
DO's	**DONT's**
Keep profiles set to private and protect tweets. Ensure all passwords are kept private and secure and change them regularly. Uphold CHA's values and ethos. Be aware of the language and content of posts – in particular where employees have an association with their employer e.g. listing their employer or linked with colleagues. Remember that social media platforms are very open and public Remember that anything posted online is permanently available and open to being published in any media.	Do not list CHA as your employer. Don't engage CHA's service users, suppliers and stakeholders via personal accounts - in order to prevent any actual or perceived conflict of interests or impropriety. Don't refer to CHA's people, activities or affairs in your postings. Don't forget that information can be passed on quickly and without your knowledge. Don't criticise, oppose or contradict CHA. Use social media to make unwelcome approaches or advances to a colleague or other person connected to CHA.
PORTABLE MEDIA/REMOVABLE DEVICES/REMOTE WORKING	
Take all reasonable care to assess the risks in the given environment and take reasonable steps to prevent the theft or loss of portable devices. When transporting, ensure that the device is safely stowed out of sight e.g. in a case or bag. Be extra vigilant in public spaces to avoid the risk of inadvertent disclosure of CHA's information to a third party - e.g. "overlooking" content displayed on screen. Log out and power off when not using device. Ensure that no unauthorised users are given access to the device or the data it contains e.g. members of family, visitors, etc. Only access secured Wireless (Wi-Fi) connections. These connections are typically announced as, and secured by, WPA/WPA2. Regularly back up data held on remote devices to the corporate system. Ensure with advice from the CSO that appropriate anti-virus and anti-spyware software is present on devices and that regular scans are carried out. In the event of loss, theft or damage, report it immediately to the CSO. The incident must also be reported to the police and a crime reference number obtained.	Do not leave portable devices unattended in a public place or in vehicles in open view - secured out of sight in the boot is acceptable, provided that there is no risk from heat/sunlight. It is not acceptable to lock the keyboard and leave the device unattended in a customer's home, public place or conference/meeting area. Always ensure you have logged out and power off the device. Store passwords on devices, write them down in an unsecured file or communicate them to any other person, even your line manager. Do not connect to the following Wireless connections: • WEP (wired equivalent privacy) secured – known to be insecure; easy to gain unauthorised access to the network. • Public Hotspots- These should be avoided due to the uncertainty of the security of the provided network. Certificate Errors – If a certificate error is displayed upon connection, then your device should be disconnected

	immediately and an alternative Wireless access point found, as the security of the connection cannot be guaranteed.