**CLYDESDALE HOUSING ASSOCIATION LIMITED**

**Policy: Remote Working Policy**

**Date: 9 December 2020**

**Lead Officer: Depute Chief Executive**

**Review Date: June 2023**

## Regulatory Standard

**Standard 3**
**The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay.**

***Guidance***

3.1 The RSL has effective financial and treasury management controls and procedures, to achieve the right balance between costs and outcomes, and control costs effectively. The RSL ensures security of assets, the proper use of public and private funds, and access to sufficient liquidity at all times.

3.2 The governing body fully understands the implications of the treasury management strategy it adopts, ensures this is in the best interests of the RSL and that it understands the associated risks.

3.3 The RSL has a robust business planning and control framework and effective systems to monitor and accurately report delivery of its plans. Risks to the delivery of financial plans are identified and managed effectively. The RSL considers sufficiently the financial implications of risks to the delivery of plans.

3.4 The governing body ensures financial forecasts are based on appropriate and reasonable assumptions and information, including information about what tenants can afford to pay and feedback from consultation with tenants on rent increases.

3.5 The RSL monitors, reports on and complies with any covenants it has agreed with funders. The governing body assesses the risks of these not being complied with and takes appropriate action to mitigate and manage them.

3.6 The governing body ensures that employee salaries, benefits and its pension offerings are at a level that is sufficient to ensure the appropriate quality of staff to run the organisation successfully, but which is affordable and not more than is necessary for this purpose.

3.7 The governing body ensures the RSL provides accurate and timely statutory and regulatory financial returns to the Scottish Housing Regulator. The governing body assures itself that it has evidence the data is accurate before signing it off.

Contents

**Introduction and Background**
Remote working is where an employee works away from their employer's location for all or part of their working week on a permanent or ad hoc basis. The practice has been around for a long time but has become increasingly popular used to promote flexibility within the workplace, attract, and retain talent within the workforce.

Remote working can be:

- An original contractual arrangement from when the employee commenced employment,
- requested by an employee as part of a flexible working statutory entitlement,
- a reasonable adjustment,
- a change in organisational culture to provide employees with choice and utilise the benefits of remote working
- implemented by Clydesdale Housing Association, following the necessary consultation and contractual change processes.

There are two types of remote working:

- **Occasional:** employees have a contractual work base (i.e. office location), but work remotely on an ad hoc basis, through informal arrangements with their team and line manager. This will extend to longer periods of time as a result of external circumstances which mean working from home is recommended by the Scottish Government for non-essential offices.
- **Contractual**: employees that work off-site as defined in their contract of employment for a specified period of their working week.

**Policy Principles**
*Clydesdale Housing Association's* Remote Working Policy aims to:

- Benefit the business from creative solutions, ideas and projects by allowing staff to do these remotely, without interruptions.
- Respond to external circumstances which necessitate working from home for a prolonged period of time
- Ensure our high level of service is maintained at all times.
- Better meet the demands of our service requirements.
- Promote our culture of inclusion.
- Integrate into and complement our health and wellbeing strategy.
- Support and embed our commitment to our environmental sustainability practices.
- Set out the parameters to ensure the above conditions are met.

**Health & Safety**
A health and safety assessment will be carried out according to *Clydesdale Housing Association's* health and safety checklist (Appendix 1), which covers VDU risks and general precautions for house-holder electrical safety. Domestic electrical supply configurations are out with the control of the employer and are the responsibility of the staff member. Employees will perform their assessment, and their line manager will then validate results during a discussion or remote visit. The employees will be expected to report any changes that may affect the arrangements in the future (in which case another assessment may be necessary).

**Occasional Remote Working**
For occasional remote working, an employee works their contracted hours from the location specified in their contract of employment. However, on occasion, it may be necessary to work remotely. This can be effective when managing certain situations such as:

- Disruptions to dependants care arrangements,
- Project work,
- Adverse weather,
- Commuting disruptions,
- An injury where the employee is fit to work but is unable to commute to their contractual work location.
- Recommendations from the Scottish Government to work from home if possible.

In all the above situations, work will be carried out effectively and efficiently with the appropriate resources, including an electronic device, e.g. laptop or tablet with sufficient broadband speed and functioning phone.

All situations for occasional remote working will be discussed individually with the employee's line manager, and they will consider the request balancing employee and business pressures and provide a decision. In the case of a recommendation from the Scottish Government which affects the entire workforce, this will be agreed by the Management Committee.

**Costs/Allowances**
Employees who on occasion work remotely will not have expenses approved for items such as for paper/ink/subsistence/internet services/wear and tear on equipment. The saving in time and money getting to/from work is a reasonable notional offset to any minimal personal costs of occasionally working remotely. However, in instances where expenses have been incurred and it would not be reasonable to expect the member of staff to pay for, receipts such be presented to the member of staff's line manager for approval. Reasonable expenses incurred for longer periods of remote working will be authorised by the member of staff's line manager.

**Contractual Remote Working**
Contractual remote working can occur in the following circumstances:

1. Making a Flexible Working Request: An employee with the required continuous service can request via their statutory entitlement to request Flexible Working.
2. Organisational Culture and Practice: Where Clydesdale Housing Association promotes regular remote working for all where it is practical, meets the needs of Clydesdale Housing Association and individual employees.

**Flexible Working Request**
Employees wishing to request remote working as a contractual arrangement can discuss the request with their line manager and follow up with a formal request in writing following Clydesdale Housing Association's Flexible Working Policy. The process outlined in the policy will be followed. Any decision to accept or reject the application will be based on Clydesdale Housing Association's business needs and requirements at the time of the request and, in line with Clydesdale Housing Association's Flexible Working Policy. Any change to the employee's working arrangement would be regarded as a permanent contractual change and therefore, must be confirmed in writing. Due to the change being permanent, a 3-6 month (depending on the nature of the role) trial period will take place first before any permanent change takes effect.

**Organisational Culture**

Clydesdale Housing Association wishes to embrace the significant benefits remote working can bring such as:

- the efficiency of performance,
- health and wellbeing of employees and,
- the positive environmental impact through reduced commuting

Clydesdale Housing Association supports a culture of remote working as a permanent contractual arrangement as long as business and service delivery needs are met and enhanced. Clydesdale Housing Association trusts its employees to fulfil their contractual obligations concerning their job role. Whether an employee is working remotely or, at Clydesdale Housing Association's location, the expectation on performance standards remains the same.

Clydesdale Housing Association believes a model of blended working is best. This means a mixture of remote and onsite working, which brings the most benefits for both business and employees. It allows for continuing face to face social interaction, collaboration, along with enjoying the benefits of remote working. For this reason, remote working will be determined by either current Scottish Government guidelines or by agreement with line managers as determined by the needs of the business.

Clydesdale Housing Association appreciates that not all employees would like to work remotely, some employees may prefer to attend the office for their working week. Any employee who wishes to continue to come to their original work location can continue to do so provided this does not contravene any Scottish Government guidelines.

Section managers will discuss with employees how remote working arrangements will work within teams and sections, including any rota for office cover and existing working patterns. Once agreed between employees and the appropriate manager confirmation will be provided in writing.

Any permanent changes to a work location is a contractual change of employment and agreement will always be sought in the first instance.

**Trial Periods**

At the end of a trial period, the arrangement will either be amended or confirmed. The decision at the end of the period will not be a surprise; this will be due to regular communication on the effectiveness of the working arrangement throughout the trial. Any adjustments can be made during the trial and can be put forward by the line manager or by employees.

**Contractual changes**

If contractual remote working has been agreed, *Clydesdale Housing Association* will write to the employee to confirm the change and any associated terms with the change.

**Costs/Allowances**

*Clydesdale Housing Association* will contribute towards remote working expenses such as:

- Reimbursing any reasonable cost that the member of staff pays for themselves such as postage or ad hoc costs which would otherwise we provided by the Association.
- Items required which are identified through a home working risk assessment.

There may be expenses that can be claimed directly by employees from HMRC. Please refer to HMRC website for the most up to date information.

**Recording the days of working from home**

All staff members must record all days worked from home on the Overview calendar in Outlook.

CHA homes reserve the right to withdraw the home working arrangement for business reasons at any time, with immediate effect.

**Travel Expenses**
Work-related travel expenses will be paid at the rate stated in your terms and conditions of employment, and as specified in Clydesdale Housing Association's Expenses policy.

**Performance Management**
Clydesdale Housing Association has a culture of trust and respect for all. Performance Management will be carried out in the same way as if employees were in the office. As in the office, if the quality or volume of work while working remotely is not at the required standard, this will be addressed via Clydesdale Housing Association's performance management process initially on an informal basis. Matters will be managed confidentially with individual employees.

**Cyber Security**

Working from home and remote system access can provide great business benefits but exposes the organisation to new risks that need to be managed. To do this the Association needs to identify and assess the risks and establish policies and procedures that support home or mobile working or remote access to systems that are applicable to users.

**What is the risk?**

Home working and remote access extends the transit and storage of information (or operation of systems) outside of the corporate infrastructure, typically over the Internet. Mobile devices may also be used in spaces that are subject to additional risks such as oversight of screens (shoulder surfing), or the theft/loss of devices.

It is important that all staff and Committee members dealing with Association business follow sound mobile working and remote access practices. To protect the organisation from risk and all users must be aware of the following risks and ensure that they guard against these at all times:

- **Loss or theft of the device:** Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.

- **Being overlooked:** Some users may have to work in public open spaces, or in premises/places where there are other people present, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.

- **Loss of credentials:** If user ID/credentials (such as username, password) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.

- **Tampering:** if the device is left unattended, an attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware. This may allow them to monitor all user activity on the device, including authentication credentials.

**Maintaining Awareness:**

All users will be trained on the use of their mobile device for the locations they will be working in. Users will be supported to look after their mobile device and operate it securely by following clear procedures. This will include direction on:

- secure storage and management of user credentials
- incident reporting
- situational/environmental awareness (the risks from being overlooked by others, etc.)

**Data Protection**

When working from home data protection can be particularly challenging. Below are some tips to help deal with this:

- Follow the Association's policies, procedures and guidance particularly the ICT Code of Practice.
- Only use technology (hardware or software) that has been approved by the Association as this will provide the best protection for personal data
- As you may be sharing your home working space with other family members always consider confidentiality and try to hold conversations where others are less likely to overhear. Where possible position your screen where it is less likely to be overseen.
- At home it is unlikely that you will have confidential waste bins. Always follow the Association's guidance or safely store print outs until you can take them into the office to dispose of them securely
- Don't mix data from the workplace with your own personal data. Ideally, all staff will be provided with secure technology to work with, however, if you are using your own device or software please ensure that this is kept separately to avoid accidentally holding data for longer than is necessary
- To avoid the loss or theft or personal data, please put paperwork and devices away at the end of the working day if possible
- Be extra vigilant about opening web links and attachments in emails or other messages. Don't click on unfamiliar web links or attachments claiming to give

you important coronavirus updates. If you receive any suspicious emails then please report these to Sabre Systems as soon as possible

- Use strong passwords, whether using online storage, a laptop or some other technology, it's important to make your passwords hard to guess.
- Communicate securely, Use the communication facilities provided to you by your organisation where available. In other words, communicate through the remote desktop which links directly to the Association's network.

More information can be found on the Information Commissioners Office website https://ico.org.uk/for-organisations/working-from-home/how-do-i-work-from-home-securely/

**Technical Support**

Clydesdale Housing Association's IT infrastructure is capable of supporting remote working and gives employees remote access to calendars, phones, e-mails and documents. Employees are required to have their broadband at sufficient speed in place. Clydesdale Housing Association will, where practical, provide the appropriate equipment and software to allow people to work remotely.

It will be required that employees have the necessary firewall and anti-virus software installed on their remote computers, to protect *Clydesdale Housing Association's* office IT system from any harm.

**Policy Review**

This policy will be reviewed in three years' time, or earlier if required by legislation.

| Approved by the Committee of Management on: | |
|---|---|
| Signed:<br>Secretary/Chairperson | Signed:<br><br>Chief Executive/Senior Staff Member |

## Appendix 1

Clydesdale Housing Association's health & safety checklist for employees working remotely. This list is not exhaustive and should be used in conjunction with section 3.20 of the Health and Safety Manual.

**Electrical Equipment**

The safety and maintenance of the domestic electrical supply/installation is the responsibility of the house-holder. Clydesdale Housing Association will only take maintenance responsibility for any equipment it directly supplies.

**House-holder checklist:**

- Ensure electrical equipment is turned off when not in use and before performing any checks
- Check plugs are not damaged
- Check domestic electrical supply is suitable for the equipment in use
- Check plugs are correctly wired and that the outer cable covering is gripped at the point it enters the plug or equipment.
- Check outer covers of equipment are sound and have no loose parts or missing screws
- Check all leads and cables routinely against damage to the outer covers
- Check for burn marks or other signs of overheating
- Repair any electrical equipment with the potential to harm
- Check and secure all trailing wires – the best way is to use power outlets nearest to the equipment. Where this is not possible tuck trailing wires securely under desks etc. and out of typical walkways
- Do not have young children unsupervised in any area where you are using electrical equipment

**Working with VDU's**

Clydesdale Housing Association's self-assessment tool will be used to ensure workstations are set up appropriately.

## Appendix 2: ICT Code of Practice

### 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**<br>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**<br>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.<br><br>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.**

## 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

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

## 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.

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.

---

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

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**:**

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] 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

3.3.4 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.

## 3.5 *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.

[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

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 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.<br><br>Close files when finished working on them to allow colleagues access and log out of the system when leaving the room.<br><br>Close down PC completely at least every week, but preferably at the end of the working day. | Divulging password to another person.<br><br>Going to lunch/meeting without closing files and logging out or locking PC.<br><br>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.<br><br>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.<br><br>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.<br><br>Ensure the subject line is meaningful and reflects content. | Using, creating or distributing inappropriate language, content[5] or material, received or sent by email; breach of Code of Conduct.<br><br>Opening attachments from unknown senders without checking if it's genuine.<br><br>Forwarding chain emails or 'humorous' messages. These have the potential to detract from work related material and cause offence.<br><br>Using email for criminal activity.<br><br>Sending unprotected personal information by email.<br><br>Don't leave subject line blank or use words like 'Hi'.<br><br>Never use all capital letters in messages or subject lines. This can be perceived as impolite or shouting. |

[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

| | |
|---|---|
| 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.<br><br>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.<br><br>Consider ‘Reply All’, do all colleagues require to be involved? Valuable resources are used every time an email is delivered to an inbox.<br><br>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.<br><br>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.<br><br>Users should ensure regular upkeep of inbox, sent items and deleted items. Systems should be employed for safe and appropriate storage of important emails. | 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.<br><br>Including large amounts of info that will need accessed at a later date within the body of an email. |

| **SOCIAL MEDIA PLATFORMS** | |
|---|---|
| **DO’s** | **DONT’s** |
| Keep profiles set to private and protect tweets.<br><br>Ensure all passwords are kept private and secure and change them regularly.<br><br>Uphold CHA’s values and ethos. | Do not list CHA as your employer.<br><br>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. |

| | |
|---|---|
| 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.<br><br>Remember that social media platforms are very open and public<br><br>Remember that anything posted online is permanently available and open to being published in any media. | Don't refer to CHA's people, activities or affairs in your postings.<br><br>Don't forget that information can be passed on quickly and without your knowledge.<br><br>Don't criticise, oppose or contradict CHA.<br><br>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.<br><br>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.<br><br>Log out and power off when not using device.<br><br>Ensure that no unauthorised users are given access to the device or the data it contains e.g. members of family, visitors, etc.<br><br>Only access secured Wireless (Wi-Fi) connections. These connections are typically announced as, and secured by, WPA/WPA2.<br><br>Regularly back up data held on remote devices to the corporate system. | 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.<br><br>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.<br><br>Store passwords on devices, write them down in an unsecured file or communicate them to any other person, even your line manager.<br><br>Do not connect to the following Wireless connections:<br><br>• WEP (wired equivalent privacy) secured – known to be insecure; easy to gain unauthorised access to the network. |

| | |
|---|---|
| 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.<br><br>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. | • Public Hotspots- These should be avoided due to the uncertainty of the security of the provided network.<br><br>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. |