CLYDESDALE HOUSING ASSOCIATION LIMITED

Policy:	Information Communication Technology Policy
Date:	31 March 2021
Lead Officer:	Chief Executive
Review Date:	March 2024
Regulatory Standard:	**Standard 4** The governing body bases its decisions on good quality information and advice and identifies and mitigates risks 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.

CONTENTS

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 it provides in communication with colleagues, residents, stakeholders and other business contacts. This Policy sets out the standards and responsibilities that support the use of ICT.

1.2 This Policy has been developed using resources made available by the National Cyber Security Centre (NCSC).[2]

1.3 This Policy and associated procedures apply to all staff and Management Committee Members of CHA (hereafter referred to as Users).

1.4 CHA will provide regular training to Users to ensure that they understand and are able to comply with this Policy and associated procedures.

1.5 Users will be required to confirm that they understand and agree to comply with the requirements of this Policy. CHA will retain records of that confirmation in accordance with the Privacy Policy.

1.6 Non-compliance with this Policy by a User may lead to action being taken under CHA's disciplinary procedures.

1.7 CHA will review this Policy and any associated procedures regularly considering equal opportunity implications and taking appropriate action to address inequalities likely to result or resulting from their implementation.

1.8 This Policy may be changed without notice in response to circumstances and threats faced by CHA. If this happens the updated Policy will be issued to Users and appropriate training provided. Individuals will be asked to confirm acceptance of the revised Policy.

2 Policy Objectives

2.1 Provide clear governance and control over CHA's ICT systems.

2.2 Control access to CHA's information systems.

2.3 Protect the security of CHA's ICT network.

2.4 Provide appropriate Disaster Recovery arrangements for CHA's ICT systems.

3 Governance and Control of ICT Systems

3.1 CHA's Management Committee has overall responsibility for ensuring that ICT Systems are appropriate, safe, secure and able to be recovered effectively should the need arise.

3.2 At an operational level, the responsibilities detailed in 3.1 are delegated to the Chief Executive (CEO).

3.3 In delivering the ICT Policy Objectives, support and guidance will be provided to Users through:

3.3.1 Providing ICT resources capable of supporting CHA's business needs and customer service requirements;

3.3.2 Effective external technical support and guidance;

---

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

[2] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

3.3.3 The design and maintenance of appropriate systems and processes relating to CHA's ICT resources;

3.3.4 Appropriate training and guidance for Users on hardware and software use;

3.3.5 Regular cyber-security skills and knowledge building.

3.4 CHA will maintain an appropriate level of insurance to cover the risks faced by its ICT resources.

3.5 CHA will use the internal audit function to test the robustness of its ICT systems and processes and check that they are being implemented effectively.

3.6 CHA will maintain Cyber Essentials certification as a minimum standard.

4 Acceptable Use

4.1 CHA will provide devices and software/apps for Users that are appropriate to their role.

4.2 User activity and use of CHA ICT resources must comply with CHA's existing policies, most notably the Code of Conducts for Committee Members and Staff, Dignity at Work Policy and our Privacy Policy.

4.3 Users must take care to ensure that their actions do not cause damage to CHA's ICT resources either accidentally or intentionally.

4.4 Use of CHA's ICT resources must be for corporate purposes, although personal use is permitted on condition that it complies with this Policy and all other CHA policy documents.

4.5 Users must always be alert to the threat of phishing scams, malware and ransomware. Staff will receive regular awareness raising sessions on how to identify and respond to these threats.

4.6 Transmission of personal data and confidential information via email will be carried out in line with CHA's Privacy Policy and data protection procedures.

4.7 Inappropriate messages are prohibited including those which contradict, oppose or infringe on the purpose, ethos or principles of CHA. Users in receipt of such messages should report this to the CEO (for staff) or Chairperson (for Committee Members).

4.8 Staff breaches of this Policy may be the subject of disciplinary or grievance procedures. Committee breaches may be the subject of procedures contained in the Protocol for Dealing with a Breach of the Code of Conduct (for Governing Body Members).

4.9 CHA will have system monitoring arrangements in place to account for user activity and identify the unauthorised or accidental misuse of systems or data.

4.10 If there is concern over a User's general conduct using ICT resources this must be raised immediately with either the CEO or Chairperson.

4.11 Users should not send potentially defamatory communication messages which criticise other individuals or organisations.

4.12 Users should not access or download inappropriate material using CHA's ICT resources.

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

5 Email

5.1 All emails sent or received through CHA's network resources are part of official CHA records. CHA can be legally compelled to show that information to law enforcement agencies or other parties[3].

5.2 CHA network resources are provided for legitimate business purposes. While respecting the privacy of individuals, CHA reserves the right to monitor User use of email and, in certain circumstances, if deemed necessary to access and record communications for business purposes which include the following (any such examinations or monitoring must be instructed by a member of the Management Team):

5.2.1 providing evidence of business transactions;

5.2.2 ensuring business procedures are adhered to;

5.2.3 training and monitoring standards of service;

5.2.4 preventing or detecting unauthorised use of CHA's network resources or criminal activity;

5.2.5 maintaining the effective operation of CHA's network resources;

5.2.6 ensuring continuity of service e.g., period(s) of staff absence.

5.2.7 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.

5.2.8 Users must not use the corporate email accounts 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.

5.2.9 Users are not permitted to use corporate email account for personal use.

5.2.10 Cyber-Security: 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.

5.2.11 Cyber-Security: Staff must always be alert to the threat of phishing scams, malware and ransomware. Staff will receive regular awareness raising sessions on how to spot these threats.

6 Internet

6.1 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. Users **must not** use any corporate systems or equipment to**:**

6.1.1 View, download, create or distribute any inappropriate content[4] or material, engage in any activities that are illegal or criminal or could adversely affect CHA's reputation;

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

[4] 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

6.1.2 Create or transmit material that might be defamatory, offensive, harassing or incur liability for CHA;

6.1.3 Broadcast unsolicited personal views on social, political, religious or other non-business-related matters;

6.1.4 Introduce any form of computer viruses or carry out other hacking activities.

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

6.3 Staff Users may use the corporate internet system for personal reasons, subject to the following:

6.4 Personal internet use should be of a reasonable level and restricted to personal time and is not permitted during work time;

6.4.1 This Policy 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.

6.4.2 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.

6.5 Cyber-Security: 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.

7 Cyber-Security

7.1 CHA will use effective and affordable ways to reduce exposure to cyber-attacks on its ICT resources.

7.2 Staff who suspect that a breach in CHA's cyber security has taken place should contact either the CEO or CSO immediately with the details. The issue will then be immediately passed to CHA's IT Maintenance Contractor. The SBRC cyber incident helpline is also available for additional support by calling 01786 437 472 weekdays 9am-5pm.

7.3 Measure employed by CHA to safeguard cyber-security will include:

7.3.1 Boundary firewalls and internet gateways – CHA will establish network perimeter defences, particularly web filtering, content checking, and firewall policies to detect and block prohibited downloads and block access to known malicious domains;

7.3.2 Malware protection – CHA has and maintains malware defences to detect and respond to attacks;

7.3.3 Patch management – CHA has systems in place to patch known vulnerabilities with the latest software versions to prevent attacks which exploit software bugs;

7.3.4 CHA has removed software download privileges from Users, except with specific permission from authorised personnel;

7.3.5 Password policy – CHA has an appropriate password policy in place and ensures that it is followed – see section 8 of this Policy for details;

7.3.6 User access control – CHA limits User execution permissions and enforces the principle of least privilege – see section 6 of this Policy for details;

7.3.7 Data storage - CHA's default position is for all data to be saved and stored on CHA's network storage resources i.e. CHA's system servers – to ensure data is backed up for security and business continuity purposes;

7.3.8 Use of removable media (portable storage devices, smartphones, digital cameras, etc) is strictly restricted to that provided by CHA.

7.3.9 Portable storage devices – the use of portable storage devices using USB ports is disabled in all CHA devices. The use of portable storage devices will only be permitted in exceptional circumstances, e.g., when connection to the network is unavailable and temporary use of such a storage drive is required to save data until it can be transferred to network storage facilities. When permitted, only CHA authorised portable storage devices can be used and these must always be scanned using anti-virus software and be encryption enabled.

7.3.10 Permission to use device storage or portable USB drives must be obtained from the CEO, upon which a Ticket should be raised with CHA's IT Maintenance Contractor for this work to be actioned. Requests to the IT Maintenance Contractor will be rejected wher proof of the CEO's authorisation is not provided;

7.3.11 User training education and awareness – CHA ensures that Users understand their role in keeping CHA secure and how to report any unusual activity;

7.3.12 CHA prohibits the use of public Wi-Fi networks on all CHA devices.

7.4 CHA will have effective plans in place to effectively deal with a cyber-attack and reduce the impact on organisational activity.

7.5 Potential internal threats will be managed through this Policy's Access Control measures and system monitoring.

7.6 System monitoring – CHA will establish system monitoring arrangements to detect cyber-attacks and account for User activity.

7.7 CHA will develop, implement and review a data back-up strategy in order to support recovery from accidental or malicious cyber-attacks.

8 Access Control

8.1 Administrator privileges will be restricted to CHA's IT Maintenance Contractor. The CEO or other staff member will only be granted these privileges in exceptional circumstances, e.g., when CHA is transitioning between IT Maintenance Contractors.

8.2 CHA enforces the principle of least privilege with Users in order to provide additional protection. This approach helps to protect against accidental or deliberate User misuse and potential damage caused by cyber-attacks where User accounts are compromised.

8.3 Staff Users 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.

8.4 User accounts are managed from creation, through-life and eventually revocation when a staff User leaves or changes role.

8.5 Staff Users are required to either lock devices or sign them off from the network when they are left unattended – staff Users are responsible for all activity on devices accessed using their credentials.

8.6 Staff User accounts are removed when employment is terminated and ICT devices recovered by CHA. Staff User accounts are temporarily suspended during periods of prolonged absence.

8.7 Committee Users will not have network privileges. They will, however, have access to CHA's secure website area which contains materials appropriate to their governance responsibilities. The CEO and Corporate Services Officer will be responsible for maintaining this resource and network resources concerning governance activity.

8.8 Committee User access to the secure website area will be removed and ICT devices provided by CHA recovered when Committee membership terminates.

9 Change Management

9.1 CHA has an inclusive culture which extends to change projects. Users will therefore be involved and consulted on all significant change projects that affect ICT resources.

9.2 CHA will develop and regularly review an ICT Strategy for the acquisition, management and disposal of network resources and its digital presence.

9.3 CHA will procure specialist advice and support in ICT change projects in order to ensure that project outcomes are achieved and that CHA achieves value for money from any investment made.

9.4 All network resources will be procured through reputable channels to ensure it is genuine.

9.5 Users will receive training and support when network resources are replaced/updated in order to ensure that this will be used effectively.

9.6 Obsolete devices will be cleared of all data and software before disposal.

9.7 CHA has removed software installation/download privileges from Users, except with specific permission from the CEO. Users requiring software installations/downloads must first obtain written authorisation from the CEO. In considering such requests, the CEO may take advice from CHA's IT Maintenance Contractor. Proof of authorisation must be presented to CHA's IT Maintenance Contractor after which a Ticket will be raised by the IT Maintenance Contractor for this work to be progressed. Failure to produce written authorisation from the CEO will result in requests being rejected.

10 Passwords

10.1 CHA requires all devices to be password/passcode protected.

10.2 PCs, laptops and tablets:

10.2.1 passwords must use of 4 or 5 random words and be at least 32 characters long;

10.2.2 use fingerprint reader/face recognition where the device supports this;

10.2.3 passwords must be unique and not used on any other device or account;

10.2.4 two-factor authentication must be used to access network resources remotely.

10.3 CHA Mobile phones:

10.3.1 access can only be obtained by using a strong password (see above), passcode or PIN/pattern lock;

10.3.2 use fingerprint reader/face recognition where the device supports this;

10.3.3 passwords/passcodes must be unique and not used on any other device or account;

10.3.4 mobile voicemail accounts must be protected by a unique PIN.

10.4 Office 365 Account:

10.4.1 Users must ensure that two-factor authentication is enabled;

10.4.2 Users must use CHA devices only to access Office 365 accounts.

10.5 Passwords/passcodes will not require routine periodical renewal as long as they comply with this Policy. However, they must be changed immediately when a User suspects that their password/passcode has been compromised.

10.6 CHA will ensure this password policy is adhered to by seeking written confirmation from Users.

11 Social Media

11.1 CHA respects the 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 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 for staff and action associated with dealing with breaches of the Code of Conduct for Committee Members.

11.2 If using social media platforms Users are expected to adhere to the following:

11.2.1 Keep profiles set to private and protect posts/tweets;

11.2.2 Ensure all passwords are kept private;

11.2.3 We do not prohibit Users from listing their involvement with CHA, however, we do advise against it;

11.2.4 Avoid personal social media connections with CHA's service users, suppliers and stakeholders;

11.2.5 Users should be aware of the language and content of their posts – in particular where Users have an association with CHA e.g., listing CHA or linked with colleagues.

11.3 Access to CHA social media administration will be controlled by the Corporate Services Officer (CSO). Users wishing content to be posted must provide appropriate media to the CSO, who will have final approval/editing authority.

12 Bring Your Own Device

12.1 CHA will provide devices and software/apps for Users that are appropriate to their role.

12.2 Staff Users are not permitted to access network resources using non-CHA devices.

12.3 The use of personal devices by Committee Users is permitted for accessing the secure website area and other non-network resources, although CHA will offer an appropriate device.

13 Remote Working

13.1 The content of this Policy applies to remote working as well as office-based work.

13.2 CHA has a separate Remote Working Policy which should be read in conjunction with this Policy.

13.3 Particular risks involved in remote working include:

13.3.1 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;

13.3.2 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;

13.3.3 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

13.3.4 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.

13.4 Users working remotely must not use public wi-fi networks as these are unsecure and highly susceptible to compromise.

14 Removable Media

14.1 Removable Media[5] 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. Users must employ good practice and take all reasonable measures to prevent loss, damage or theft.

14.2 Staff Users must use PIN or Password protection on smartphones and on CHA voicemail accounts.

14.3 Smartphones must have encryption enabled in order to protect data in the event of the device being stolen or lost.

14.4 Smartphones must also have remote tracking enabled - this means that if the device is lost or stolen, it can be remotely tracked and erased.

14.5 Users may only use CHA removable media with CHA 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 not be connected to CHA devices.

14.6 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.

14.7 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.

14.8 Any removable media used by staff 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 removable media. 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.

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

14.9 If a Staff User is provided with removable media in order for them to be contactable then it should be turned on at all times during business or 'on-call' hours, except when driving or when the User deems it inappropriate due to work reasons, e.g., when in a meeting.

14.10 For User protection, all removable media should have location software enabled, this must not under any circumstances be disabled.

14.11 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.

14.12 Access to CHA network resources 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 CHA network resources.

14.13 When taking digital images or audio recordings it is important to consider responsibilities regarding privacy; the security of the image; professional responsibilities and legal obligations. Please refer to CHA's Privacy Policy for details.

14.14 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 Users are concerned or unsure how to secure digital images or audio recordings in this way, please contact the CSO for further advice.

15 Collaboration Services & Systems

15.1 CHA only authorises the use of Zoom, Microsoft Teams and Horizon PC Softclient Collaboration as collaboration services and systems for CHA's people.

15.2 Zoom - Always enable the 'Waiting Room' in Security settings and require participants to enter a passcode before entering the meeting.

15.3 Video conferencing protocols:

15.3.1 Always use a headset & microphone provided by CHA;

15.3.2 Be aware of your surroundings in order to minimise the risk of unauthorised persons overhearing discussions that could constitute a breach of GDPR;

15.3.3 Use the mute facility whenever you are not speaking in order to minimise background noise for other users and improve audio quality.

16 DECLARATION

I ……. confirm I have read and understood the terms of the ICT Policy and I agree to uphold its requirements in all my activities associated with Clydesdale Housing Association.

I understand that if I am found to have breached any points mentioned in this ICT Policy or acted against its spirit, action will be taken in accordance with the Protocol for dealing with breaches of the Code of Conduct (for Committee Members) or disciplinary procedures (for staff) and could ultimately result in my removal from the Management Committee or dismissal from employment.

Signed ……

Date ……

Appendix 1: Practical Do's & Don'ts

INFRASTRUCTURE/SOFTWARE	
DO	**DON'T**
Create a unique system password that complies with CHA's password policy. Close files when finished working on them to allow colleagues access and log out of the system every time you leave your device unattended. Restart devices at least every week, but preferably at the end of the working day in order to update software patches	Divulge passwords to another person. Leave your device until it has been locked or you have signed out.
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. Report any suspicious emails to the CEO and CSO immediately. 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. 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. Users should ensure regular upkeep of inbox, sent items and deleted items. Systems should be employed for safe and appropriate storage of important emails.	Use, create or distribute inappropriate language, content[6] or material, received or sent by email. Open attachments from unknown senders without checking if it's genuine. Forward chain emails or 'humorous' messages. These have the potential to detract from work related material and cause offence. Use email for criminal activity. Send unprotected personal information by email. Leave subject line blank or use words like 'Hi'. Use all capital letters in messages or subject lines. This can be perceived as impolite or shouting. Send files greater than 10MB in size via email, this could 'block' the mail exchange as the file size is considered excessive. Enquire with Corporate Services Officer for alternative solutions. Include large amounts of info that will need accessed at a later date within the body of an email.

[6] 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

SOCIAL MEDIA PLATFORMS	
DO's	**DON'T**
Keep profiles set to private and protected. 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.	List CHA as your employer. Engage CHA's service users, suppliers and stakeholders via personal accounts - in order to prevent any actual or perceived conflict of interests or impropriety. Refer to CHA's people, activities or affairs in your posts. Forget that information can be passed on quickly and without your knowledge. Criticise, oppose or contradict CHA. Use social media to make unwelcome approaches or advances to a colleague or other person connected to CHA.
REMOVABLE MEDIA/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.	Leave 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. Leave the device unattended in a customer's home, public place or conference/meeting area. Store passwords on devices, write them down in an unsecured file or communicate them to any other person, even your line manager. 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.