Information, Communication & Technology Policy

Date of Review: 10.03.22

Date of Approval: 28.03.22

Date of Next Review: March 2025

Craigdale Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

Information, Communication & Technology Policy (ICT)

Contents **Page No**

Information, Communication & Technology Policy

Introduction

Information, Communication & Technology is critical to Craigdale Housing Association to allow us to deliver our services.

Information, Communication & Technology (ICT) is about making sure that all the information we encounter at Craigdale – whether it's about people or the association – is handled properly throughout its life cycle. This means that all information must be collected, stored, used, shared and disposed of appropriately and securely, by following legal requirements and best practice.

Purpose

The purpose of this Policy is to set out the principles that the association will observe to meet its organisational and legislative requirements with regards to how we handle information.
The overall aim of the policy is to:

- have accurate, up-to-date and reliable information, readily available when needed to deliver services and support decision-making
- have improved compliance and reduced risk
- have staff who understand the importance of good information governance
- increase staff productivity
- improve customer service; and
- give customers confidence in our ability to handle information with transparency and security.

Scope

This policy applies to all information, in any format, including paper and electronic copies, created, received and maintained by Craigdale.

The policy applies to all staff, board members and suppliers' of Craigdale, who may create, receive or have access to Craigdale information.

The policy applies to all locations where information is created, received and used, including the office, home and remote use.

Principles

1. We will value our Information

Information will be identified and valued as an asset and will always be used to its full potential by ensuring we understand the information the association holds and how it needs to be used to support the services we provide.

2. We will comply with legislative and regulatory requirements
Craigdale is committed to continuously improving the way it responds to requests for information under statutory access, including Subject Access and Environmental Information requests. Information tenants require about Craigdale on how and why it makes decisions and the services it provides will be easily accessible.

3. We will handle information securely
Information is stored, managed and protected in a manner that reflects its value throughout its lifecycle.

4. We will have quality information that is fit for purpose
Accurate, up-to-date relevant and reliable information is readily available when needed to deliver services and support decision-making.

5. We will have good Records Management
By implementing best practice frameworks for Records Management, Craigdale will ensure that effective processes are in place to manage all records, from creation through to disposal.

Responsibilities

The Chief Executive Officer (CEO) has ultimate operational responsibility for Craigdale's policy in respect of ICT, considering legal and regulatory requirements.

The Senior Corporate Services Officer is responsible for overseeing ICT daily, developing and maintaining policies, procedures and guidance. The Senior Corporate Services Officer will coordinate compliance across Craigdale and provide continuous awareness of best practice.

Senior Officers are responsible for ensuring that the policy and any supporting procedures and guidelines are built into operational procedures and that there is continuous compliance.

All staff and board members are responsible for ensuring that they are aware of the requirements placed on them and that they comply with these daily.

Training and Awareness

Craigdale acknowledge that training and awareness plays a vital role in creating a culture which takes ICT seriously.

Craigdale will ensure:

- Mandatory ICT training is in place and accessible to every member of staff.
- Regular ICT communications are disseminated internally to encourage good ICT and to continually raise awareness
- ICT advice and support is easily accessible for all staff.

Related Policies and Procedures

This policy is linked and supported by the following policies:

- Data Protection Policy
- Retention of Records Policy & Schedule
- Business Continuity & Disaster Recovery Plan

Key Regulatory Requirements

Legislation that places specific information governance and record keeping obligations on how Craigdale handle information includes, but is not limited to:

- Housing (Scotland) Act 2014
- UK General Data Protection Regulation 2018
- Data Protection Act 2018
- Environmental Information (Scotland) Regulations 2004
- Freedom of Information (Scotland) Act 2002 *(proposed to be enforceable from April 2019)*
- Computer Misuse Act 1990
- Privacy and Electronic Communications Regulations 2003
- Human Rights Act 1998
- Payment Card Industry: Data Security Standard (PCI-DSS)

Monitoring

Compliance with this policy will be monitored on a regular basis and reported to the Board annually.

Information Systems Security Policy

Introduction

The continued confidentiality, integrity and availability of information systems underpin the operations of Craigdale Housing Association (Craigdale). A failure to secure information systems would risk the ability of Craigdale to deliver its services to tenants effectively.

This Information Systems Security policy provides the guiding principles and responsibilities of all staff required to safeguard its information systems. This forms part of a framework of policies under the ICT Policy.

It is important that all staff are aware of and carry out their own personal responsibilities to ensure the security of Craigdale IT and communication systems.

Purpose

The purpose of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned by Craigdale.

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day-to-day business.
- Protecting information assets under the control of the organisation.
- Safeguard the reputation of Craigdale by ensuring its ability to meets its legal obligations and to protect it from liability or damage through misuse of its IT facilities

Scope

This Information Systems Security Policy applies to all staff and board members who have access to Craigdale information, and all the systems used to store or process it.

Principles

Information security follows three overarching principles:

- **Confidentiality**: Information is only seen or used by people who are authorised to access it.

- **Integrity**: Any changes to information by an unauthorised user are impossible (or at least detected), and changes by authorised users are tracked.

- **Availability**: Information is accessible when authorised users need it.

This policy incorporates these principles to all information to ensure continuity of operation of Craigdale's information systems and to reduce the risk of damage from security incident.

Responsibilities

All staff who works for Craigdale have a responsibility for complying with this policy when handling information and information systems. Staff are also responsible for reporting any security incidents promptly.

The following roles have key areas of responsibility:

The CEO is responsible with support from Senior Corporate Services Officer for:

- Managing information security
- Monitoring standards and advising on security issues
- Managing investigations of Security Incidents

Physical and Environmental Security

All ICT and network equipment will be physically secured with appropriate access control in place to ensure that only authorised personnel have access.

Wherever practical, equipment must be sited in a suitable environment to prevent loss, damage, or compromise of service and interruption to organisational activities.

All persons accessing Craigdale premises should wear or be prepared to produce on demand Staff ID cards/ identification.

Controls should be adopted to minimise the risk or potential threats to the physical equipment including theft, fire, dust, liquid damage, electrical interference or failure, chemical effects or environmental hazards.

Network

The Craigdale network will be protected by key controls such as Firewalls, Intrusion Prevention System, Mail and Web Filtering, Anti-Virus, VPN, Access Control Lists as well as further underlying security controls to prevent the network from both internal and external threats.

Access Control

<u>Creating, Controlling and Managing User Accounts</u>

Written procedures for access control and passwords based on business and security requirements will be in place for all systems.

Users should only have access to the systems they are authorised for, access to information systems should be granted on a "need to know and auditing access" basis and consider access rights, associated privileges and be authorised in accordance with the system owners. Access to privileged accounts and sensitive areas should be restricted. Users should be prevented from accessing unauthorised information.

Password procedures should contain password requirements such as frequency of change, minimum length, character types which may or must be utilised and regulate password storage for each system.

Users should have unique combinations of usernames and passwords and are responsible for any usage of their usernames and passwords. Users must keep their passwords and system passwords confidential and not disclose them.

Remote access to Craigdale's network and systems is permitted under business continuity by the Senior Management Team and for the Senior Management Team to work occasionally from home to support our business requirements.

Granting System Access

Requests for a user account, access privileges and email system access must be granted only by a clear chain of authority. Approval must be obtained from the CEO before a system administrator grants access privileges.

The ability to create and allow access to servers, services or applications is limited to staff with relevant authority. System and network privileges of all users, systems and programs must be restricted to the lowest level required to meet business needs.

On written (Email) application of appropriate senior officer, user accounts and associated privileges will be suspended immediately.

All user accounts must be disabled on termination of employment.

Password Control

The following password measures should be implemented on all Craigdale systems and networks:

- All server accounts must be password protected; user account passwords may not be shared with or revealed to anyone. Different passwords will be used for different systems.
- User account passwords must not be written down and left in a place where unauthorised persons might discover them.
- Passwords should be set in line with the Password Policy
- All vendors supplied generic accounts and default passwords must be changed.
- Non-personal accounts must be assigned to a named person, who will be held responsible for that account and should maintain an audit trail of said account.
- No employees leaving the organisation on termination of employment should retain access to non-personal accounts, account passwords should be changed.
- Multi-user accounts and passwords must not be used unless strict password management is in place.
- System accounts and passwords should be secured and used only in emergencies.
- All passwords must be changed immediately if they are suspected of being disclosed or known to have been disclosed to anyone.

Monitoring of System Access and Usage

Access and use of ICT systems will be logged and monitored in order to detect unauthorised information processing activities. Usage will be traceable and auditable to a specific entity, e.g., a person or a specific system.

The IT Provider should register substantial disruptions and irregularities of system operations, along with potential causes of the errors. Capacity, uptime and quality of the ICT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.

Craigdale reserve the right to intercept any form of electronic communication made on Craigdale systems in line with the following:

- Gaining routine access to business communication
- Monitoring standards of service and training
- Preventing or investigating criminal activities
- The malicious use of the ICT system

Craigdale monitors the performance and integrity of the system on a continual basis and reserves the right to withdraw access to the system if abuse or misuse is taking place.

External Third-Party Access to ICT Assets

External parties include customers, consultants, auditors, developers and suppliers. ICT Assets include information (databases, data files, etc.), software, hardware (including removable media) and services.

No third-party ICT equipment must be connected to the Craigdale network without explicit consent from the CEO with support from Senior Corporate Services Officer.

Access to Craigdale network, servers, or information systems by third parties must be controlled. Access requirements of any third party will be risk assessed by the CEO with support from Senior Corporate Services Officer. Access provided to third party organisations must have formal agreements or contracts in place.

Third party accounts must be configured to automatically disable after the period defined in the contract.

Protecting Information, Backup and Encryption

Protecting Information

Users of the PCs and Laptops where possible should always save data to a network share. Users are not permitted to save data to the local PC hard disk where no back up may exist and hard disk failure may occur.

All Craigdale servers must be served by or fitted with a suitable back up device.

Changes to network configuration (IP number, Machine name etc.) must only be carried out by the IT Support Provider.

Local PC administrator accounts must not be disclosed to staff. Changes to PC administrator accounts must only be carried out by the IT Support Provider.

The IT Support Provider must ensure the documentation of physical and virtual servers, services hosted, protocol usage and available ports must be in the possession of relevant core administrators.

Firewall technology must be made available and utilised on systems identified as requiring such a level of security.

All computers, ICT equipment and servers connected to the Craigdale network where applicable must run a version of the Operating System and installed applications with the latest available security patches and updates, all computers and servers must have approved and up to date virus-scanning software enabled. Users must notify the CEO and the IT Support Provider immediately if they suspect their PC/laptop has become infected. Any PC service or system suspected of being infected must be isolated from the network immediately.

Appropriate technical and organisational controls for physically securing media including but not limited to computers, removable electronic media, receipts, paper reports, and faxes to prevent unauthorised persons from gaining access to personal data, cardholder data or commercially sensitive data must be in place.

Cardholder and personal data are susceptible to unauthorised viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal and cardholder data and against accidental loss or destruction of, or damage to such data.

Backups and Recovery

Ensuring adequate controls and procedures are in place for the backup of Craigdale data is the responsibility of the CEO with support from Senior Corporate Services Officer involved in the back-up process.

All sensitive or confidential, valuable, or critical information saved on Craigdale computer systems and networks must be regularly backed-up.

Back-ups for critical business functions should be stored off-site in suitable secure conditions.

Back-up and recovery procedures must be documented and tested. Operation logs must be maintained and be subject to regular independent checks.

Encryption

Storage and transfer of personal data defined by the Data Protection laws and commercially sensitive Craigdale information should be encrypted, or password protected.

Information Security Incident Management

All Information Security Incidents must be reported to the CEO or Senior Corporate Services Officer promptly as per the Security Incident and Breach Reporting Procedure.

Acceptable Use / Internet and e mail

Craigdale have a separate Acceptable Use of ICT systems policy.

Training

All staff will be aware of good practice in information security.

Adequate and role specific training will be provided to everyone who must handle information and information systems to ensure they understand their responsibilities when working with these.

Breach of Policy

Any breaches of this policy may be considered under Craigdale's disciplinary procedures, and may result in disciplinary action being taken, including dismissal.

Monitoring and Reporting

Regular audits will be undertaken to check compliance with the law, this policy and any related information security procedures.

Severe risks resulting from Information Security Incidents will be recorded on the Corporate Risk Register.

All procedures and guidance will be reviewed on a regular basis to ensure they meet regulatory requirements and best practice.

Acceptable Use of ICT Systems Policy

Introduction

Craigdale Housing Association (Craigdale) aims to help staff and board members make the best use of the ICT systems and facilities. The use of ICT can bring significant benefits to the work staff and board have to carry out to delivery our services. However, it can also introduce significant types of risk to the association. This policy forms part of a framework of policies under the ICT Policy.

Purpose

The purpose of this policy is to provide a safe framework for using ICT without exposing Craigdale or our staff and board to the risks which can come with its use.

This Policy aims to:

- Ensure acceptable use of ICT by all users.
- Establish the parameters of appropriate use and best practice.
- Protect Craigdale and users from potential legal liabilities.

Scope

This Acceptable Use of ICT Systems Policy applies to all staff and board members who have authorised access and use of Craigdale ICT systems and services.

The policy covers the use of:

- All computers, laptops and tablets
- All telephone systems, including faxes and mobile phones
- All IT systems and software, including email and internet access

Unacceptable Use

Craigdale ICT systems may not be used directly or indirectly by staff or board members for the download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
- unsolicited “nuisance” emails
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of another member of staff or a third party
- material which promotes discrimination based on race, gender, religion or belief, disability, age or sexual orientation
- material with the intent to defraud or which is likely to deceive a third party
- material which advocates or promotes any unlawful act
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
- material that brings the association into disrepute.

Craigdale ICT systems may not be used directly or indirectly by staff or board members for the purposes of:

- intentionally wasting Craigdale resources
- corrupting, altering or destroying another User's data without their consent
- disrupting the work of other Users or the correct functioning of the Association's Network; or
- denying access to Craigdale's network and its services to other users.
- pursuance of commercial activities

No staff or board member should:

- introduce data-interception, password-detecting or similar software or devices to the network
- seek to gain unauthorised access to restricted areas of the network
- access or try to access data where the user knows or ought to know that they should have no access
- carry out any hacking activities; or
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

Staff and Board are made aware that e-mails, internet usage and any electronic communication can be monitored.

Personal Use of ICT

Personal use of ICT, including email and internet is permitted outside of your working hours, so long as this does not interfere with the performance of expected duties. As a general principal access to e-mail and the internet via the Association's resources will not be available out with office hours except where prior permission has been sought and granted.

Breach of Policy

A Senior Officer concerned about an employee's or board members potential violation of the Association's acceptable use policy (for example, excessive use of e-mail for personal use, frequently shopping or using social media in working hours) should not singly seek to gain access to a user's electronic communications, instead, the Senior Officer should:

- review whether expectations and standards in this area have been well communicated and made clear to the user,
- pursue direct communication with the user regarding the issue,
- proceed as one would handle any personnel-related disciplinary action.

Password Policy

Introduction

Craigdale Housing Association (Craigdale) recognises the requirement for a robust password policy which is appropriately structured, implemented and reviewed. Passwords are an important aspect of information security and can be the first line of protection for staff user accounts.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all staff who have or are responsible for any user accounts (or any form of access that supports or requires a password) on any ICT system owned or operated by Craigdale.

Responsibilities

All staff are responsible for taking the appropriate steps to meet the requirements of this policy when selecting and securing their passwords.

Enforced Password History

This security setting determines the number of unique new passwords that must be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords. This policy enables administrators to enhance security by ensuring that old passwords are not reused continually.

To maintain the effectiveness of the password history, we do not allow passwords to be changed immediately after they were just changed by also enabling the Minimum password age security policy setting

Craigdale Housing Association currently has this set to **24 passwords** before you can reuse an old password.

Maximum Password Age

This security setting determines the period (in days) that a password can be used before the system requires the user to change it. Note that the maximum password age is between 1 and 999 days, therefore the minimum password age must be less than the maximum password age.

Note: It is best practice to have passwords expire every 30 to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to crack a user's password and have access to your network resources.

Craigdale Housing Association currently has this set to **90 days** before you are asked to change your password.

Minimum Password Age

This security setting determines the period (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days.

Craigdale Housing Association has this set to **1 day** before you can change your password.

Minimum Password Length

This security setting determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters.

Craigdale Housing Association has this currently set to **9 characters.**

Passwords Complexity Requirements

This security setting determines whether passwords must meet complexity requirements.

If this policy is enabled, passwords must meet the following minimum requirements when they are changed or created:

- Not contain significant portions of the user's account name or full name
- Be at least six characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Important: Complexity requirements are enforced when passwords are changed or created.

Default: Enabled on domain controllers
Disabled on stand-alone servers

Craigdale Housing Association has this currently set to **Enabled.**

Store Passwords Using Reversible Encryption

This security setting determines whether the operating system stores passwords using reversible encryption. This provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

This policy is required when using Challenge-Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Services (IAS). It is also required when using Digest Authentication in Internet Information Services (IIS).

Default: Disabled.

Craigdale Housing Association has this currently set to **Disabled.**

Review & Monitoring

The password policy is defined through server group policy management and therefore once implemented requires no user intervention to administer and monitor.

Our IT Support Company will review and verify status on this annually each January.

N.B. If you require the policy to be verified out with the normal review process to assist with pre-audit preparation this can be carried out on request.

List Usernames & Passwords

We do not keep list of users and passwords even in secure location. The System Administrator can reset any password and the existence of a list undermines the group policy control of the password procedure. In addition, the frequency of change normally dictates that any list is frequently out of date which would contravene the policy procedures.

Staff Password Privacy

Staff are not permitted to share passwords with anyone, including line managers or IT Support Providers.

Staff should not:

- reveal a password over the phone to anyone
- reveal a password in an email message
- hint at the format of a password (e.g., “my family name”)
- reveal a password on questionnaires or security forms
- share a password with family members
- use the "Remember Password" feature of applications
- write passwords down
- store passwords in a file on ANY computer system unencrypted.

If someone demands a password, refer them to this policy and direct them to contact the CEO.

If an account or password is suspected to have been compromised, report the incident to the CEO and IT Support Provider as soon as possible.

Staff Exit Policy

Staff exit procedure includes instruction to IT Provider to initially change the user password and redirect email. Accounts will be deleted after three months.

Board Exit Policy

Board Members who resign from the Board and who have IT equipment i.e., laptops, netbooks, tablets or mobile phones devices must return these items to the Senior Corporate Services Officer along with log-in details so the device can be wiped.

Social Media Policy

Introduction

Craigdale understands that social media tools are changing the way we work, interact and socialise. We all have access to social media tools and the ease of access to the web means that people make use of these sites to keep in touch with friends and colleagues. Social media is a great way to engage and communicate, but there are also potential risks that we must all be aware of. It is important that you are aware that information posted on these sites is public and may be viewed by colleagues, customers or the media.

Purpose

This policy sets out responsibilities for the use of social media by our employees and Board members to protect Craigdale, our tenants and colleagues from inappropriate or unacceptable use of social media. The policy also introduces a set of principles which everyone is expected to follow when using social media.

The overall aims of this policy are to enable everyone:

- to understand their responsibilities when using social media and what should, and should not, be written or posted
- to highlight the potential risks involved when posting on a social media site
- to understand the implications of using social media inappropriately

Definitions

Social Media
Social media is a set of online tools used to communicate and engage with other people and includes:

- profile pages or groups on social networking sites e.g., Facebook, LinkedIn
- micro-blogging e.g., Twitter
- writing blogs or commenting on other people's blogs
- participating in conversations on public and private web forums
- participating in online votes and polls
- reviewing products or services on retailer or service provider websites
- photo or video sharing sites e.g., Flickr, Instagram, Snapchat, Tik-Tok, YouTube; Tenant.net

This list is not exhaustive, as social media is a constantly evolving and the types of social media available may change over time.

Personal Social Media
Any social media accounts setup and used by employees or Board Members in their own time using their own personal details. These accounts are linked to personal (non-Craigdale) email addresses.

Personal Use of Social Media

Those who use social media in their personal life should be mindful that, while they are not acting on behalf of the association, the inappropriate use of social media may damage their own reputation and that of Craigdale, if they are recognised as being one of our employees.

If you identify your association with Craigdale – for example, by stating that you work or by posting pictures of yourselves at work - and/or discuss your role, you are expected to behave professionally, and in a way that is consistent with Craigdale's values and policies.

Even if you do not directly associate yourself with Craigdale, your link with the association can become known through images on friends' sites or on the Craigdale website, or by someone searching for names via internet search engines.

Any communications that you make in a personal capacity through social media must not:

- bring the association into disrepute,
- breach confidentiality of an individual or disclose confidential information you obtain in the course of your work,
- do anything that could be considered discriminatory against, or bullying or harassment of, an individual.

Principles

Everyone must be aware that they are responsible for any comments they make on a blog or social networking site. When using these sites Craigdale expects you to consider carefully what you post onto these sites and to follow the principles outlined below:

1. **Only use social media in your own time**.
   You must not use personal social media sites during your working hours. Craigdale does not permit access to social media websites from the association's computers or devices during normal working hours, however, permits usage of your own device during lunch breaks, if this does not interfere with association operations.

   You must also limit your use of social media on personal devices e.g., mobile phones, to the same times as outlined above.

2. **Only use personal email accounts for personal social media accounts**.
   Do not use any "@craigdaleha.co.uk" email addresses when setting up personal social media accounts.

3. **Make clear opinions are your own.**
   If you choose to associate yourself with Craigdale you must make it clear that any views/opinions/comments posted are your own, and not those of Craigdale. A disclaimer could be used to make it clear that opinions expressed are solely those of the author and do not represent the views of Craigdale e.g. *"The views expressed on this site are my own and don't reflect the views of my employer"*

   The use of a disclaimer, however, does not override the need to follow other principles in this policy.

   Be careful when sharing or re-tweeting posts, as they could be seen to be endorsing someone else's point of view

4. **Respect the confidentiality of Craigdale information.**
   Do not post any personal or confidential association information about Craigdale tenants, colleagues or the association itself.

   Unless originally intended for communication to the public, do not post information you have learned in the course of your role.

5. **Social Media - Do not follow, friend or link with tenants**.
   Allowing a person who uses Craigdale services (i.e., tenants or residents), their carer or family member to be your online friend or follower is not acceptable. This creates a personal relationship outside of the workplace and leaves both you and people who use our services open to allegations from any comments they may post. (This is in line with the SSSC Guidance in relation to use of social media.)

6. **Respect others privacy and feelings.**
   How you behave on social media should be the same as how you would behave in your Craigdale role, it should not breach the Code of Conduct.

   You should seek permission from colleagues before posting personal details or images that may link them with Craigdale and should not post anything about someone if they have asked you not to. You must always remove information about a colleague if you have been asked to do so.

   - You should not post images or make comments which are discriminatory or could amount to bullying or harassment.
   - You should not post comments about colleagues or other people you encounter at work (even if you don't name them) as other people may still be able to work out who you are referring to.
   - Do not post images containing customers on personal social media accounts. This does not prevent you sharing, re-tweeting or linking to images that have been published on official Craigdale sites.
   - You must not post information or make comments that cause embarrassment or offence to Craigdale, colleagues or tenants.

7. **Be careful when talking about Craigdale-related issues.**
   Social media sites are a great way to share your thoughts, but sometimes there are more appropriate channels, particularly if you are not happy with something at Craigdale. If you have an issue with a colleague, manager or something that Craigdale has done, there are internal channels that you can use, including speaking to your senior officer or CEO.

8. **Communicate as yourself.**
   If you choose to associate yourself with Craigdale via your social media site, you are expected to post under your real name. This demonstrates openness, honesty and accountability.

   If you post under a pseudonym and at a later stage these posts are associated with your real name, all previous posts will be admissible if required for any disciplinary investigation.

9. **Be aware of how online posts are, or can become, public.**
   You should be aware of privacy limitations when posting material using social media, and the extent to which information can be in the public domain. Whatever is posted on a social media site could be in the public domain immediately or, if initially shared with a limited group of followers or friends, could still be copied and shared or published elsewhere.

   You are advised to carefully consider what you want to say before you publish anything, and work on the basis that anything you write, or post could be shared more widely without your knowledge or permission.

   You are advised to configure your privacy settings and review them regularly because social media sites cannot guarantee confidentiality and do change settings regularly.

10. **Ensure all posts are legal**.
    Be careful that what you post does not break the law.

    Remember that **you** are legally liable for anything you write or post online

    You must not post any commentary, content, or images that are defamatory, pornographic, harassing, offensive, which can create a hostile work environment or that, may bring Craigdale into disrepute. You could also be prosecuted by an individual or organisation that views your commentary, content, or images as defamatory, pornographic, harassing, offensive or creating a hostile work environment.

    Ensure you do not infringe any copyright rules.

11. **Remember the Internet never forgets.**
    What you publish could be widely accessible and be around for a long time, so consider the content carefully. Google has a long memory, and the internet never forgets, even if you think that a post has been deleted.

    Google yourself. If you want to engage in social media or have done for some time, it is always worth understanding what information, images and content is on the web that refers directly to you.

12. **Do not set up Craigdale sites or groups.**
    No employee should set up corporate sites without the authorisation of the CEO.

    You must not set up sites that are made to resemble an official site, use Craigdale logos anywhere on your social media sites, or copy photos from Craigdale's website.

Inappropriate Use of Social Media

Anyone who becomes aware that someone is conducting themselves on a social media site that is potentially detrimental to Craigdale or out of line with this Social Media policy should inform a Senior Officer as soon as possible.

If you are concerned that you have made a mistake or error of judgement regarding something you have posted on social media that is included in this policy or could be potentially detrimental, let a Senior Officer know as soon as possible.

Do not ignore mistakes – the sooner it is addressed, the more likely the impact will be reduced.

Use of Social Media at Work

The use of social media sites via Craigdale ICT equipment can be monitored and any excessive usage may be investigated by Senior Officers. You should be aware that use of social media using Craigdale ICT equipment or personal devices during working time is not permitted and may be considered a disciplinary offence.

Breach of Policy

Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, which would include but are not limited to incidents of bullying of colleagues or social media activity causing serious damage to the association, may constitute gross misconduct and lead to summary dismissal.

Secure Remote Working Policy

1.0 Overview

1.1 Remote working is becoming commonplace in many businesses. It allows flexibility for both personnel and the business, allowing employees to work from home or on the go. It is essential, however, that remote work does not expose the business network, data or devices to unauthorised access or malicious software.

1.2 A Secure Remote Working Policy sets out rules and guidelines on remote work, helping personnel protect their devices and data and the business network while working away from the business premises.

2.0 Purpose

2.1 The purpose of this Secure Remote Working Policy is to help personnel work securely when away from the business premises, and to protect the business network, devices and data from unauthorised access and malicious software.

3.0 Scope

3.1 This policy covers all employees, consultants, contractors and other affiliated personnel who use the business' devices or connect to the business' network when away from premises owned or controlled by the business.

4.0 Policy

4.1 Any devices containing or accessing the information resources at Craigdale must be approved by the CEO or Senior Corporate Services Officer prior to connecting to the information systems of the Association, whether the devices are owned by the Association or not.

4.2 Employees working remotely must take all reasonable measures to protect the devices from loss, theft, and unauthorised access.

4.3 Any mobile computing or storage devices that contain sensitive or confidential Craigdale data must protect that data with encryption and a password.

4.4 When company data on mobile computing or storage devices is not in use on or from those devices in ten working days, it must be removed from those devices.

4.5 Databases and other Association data which resides on the Associations network or on Association's computers, shall not be downloaded to mobile computing or storage devices without written approval from the CEO.

4.6 Any lost or stolen mobile computing or storage devices must be reported to the IT Team and line manager without any undue delay.

4.7 Any unauthorised access to a mobile computing or storage device or to the data contained within must be reported to the IT Provider or a line manager without any undue delay.

4.8 Personnel should avoid connecting to Public Wi-Fi services whenever possible, and when required to do so they should ask for advice from the IT Provider on the use of VPNs and other security measures to help protect business data from exposure on insecure networks.

4.9 Any devices accessing business networks or data must be protected with antivirus software approved by the business' IT Provider.

4.10 Any device accessing business networks or data must have automatic logout enabled after a period of no more than 5 minutes of inactivity.

4.11 Personnel should ensure that they access business networks and data only from places where no one can potentially see or take images of screens showing company data.

5.0 Compliance

5.1 Compliance Measurement

The CEO will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exceptions to this policy must be approved by the CEO in advance and have a written record.

5.3 Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Policy Review

This policy will be reviewed every three years, and in accordance with the following on an as and when required basis:

- Responding to any new legislative changes; and
- good practice guidance
- to address any weakness in the policy that has been identified as a result of a security incident

Approval

This policy was approved by the Board on Monday 28th March 2022.

Appendix A

Software Used within the Craigdale Housing Association

Name	Function	Users
SDM	Rents & Housing Management	All Staff
SDM	Waiting List & Allocations	All Staff
SDM	Repairs & Maintenance	All Staff
SDM	Complaints	All Staff
SDM	Dashboard	All Staff
SDM	Nominal Ledger	Snr Corporate Services Officer & Finance Services
SDM	Purchase Ledger	CEO, Snr Corporate Services Officer, Snr Housing Services Officer, Maintenance Services Officer & Finance Services
Sage 50	Sales Ledgers	Snr Corporate Services Officer & Finance Services
Sage 50 Payroll	Payroll and minor HR recording	Currently outsourced to FMD Financial Services
Hub	Planned Maintenance	CEO, Maintenance Services Officer, Maintenance & Finance Services
Microsoft Office	Office automation functions	All staff
Internet browser	Internet usage	All staff
Outlook	e-mail system and calendar	All staff
Internet Banking	Check account balances, transfer funds between accounts	CEO, Snr Housing Services Officer, Snr Corporate Services Officer & Finance Services
Internet Banking	Transfer funds to Suppliers	CEP, Snr Corporate Services Officer & Finance Services
Allpay		Snr Housing Services Officer & Housing Services Officer
Filezilla	Housing Benefit statements	Snr Housing Services Officer & Housing Services Officer
Adobe reader	pdf file reader	All Staff
Vipre Endpoint Security & Solar Winds MSP	Virus protection	All Staff
Zoom	Virtual Meeting Provider	All Staff
Dropbox	Portal used to transfer large files	All Staff

Appendix B

STAFF MEMBER AGREEMENT

I confirm that I have read and understood Craigdale Association's ICT Policy.

I accept that my failure to comply with the rules set out in this Policy may result in suspension of access, disciplinary and/or legal action pursued against me as per my Terms of Conditions of Employment.

DATE:	_____
NAME:	_____
SIGNATURE:	_____

BOARD MEMBER AGREEMENT

I confirm that I have read and understood Craigdale Association's ICT Policy.

I accept that my failure to comply with the rules set out in this Policy may result in suspension of access, referral to the Board and/or legal action pursued against me.

DATE:	_____
NAME:	_____
SIGNATURE:	_____