# Scope

The policy applies to all staff, contractors and others working at Retirement Capital who have access to IT systems and services provided by the Company.

It applies to any device connected to any company network.

It applies to any device owned by the Company.

# Responsibilities

All mobile workers, i.e. those who work in public places or while travelling are responsible for adhering to this work instruction.

# Work Instruction

# Internet Usage

The Company recognises that many business procedures and activities require internet connection and that it is common practice for individuals to use the internet for personal activities.

* Personal use should not interfere with business functions and should be kept to a reasonable level and restricted to non-work times, such as breaks and during lunch.
* Personal internet usage includes the use of Smartphones and other personal devices for social networking, text message and telephone calls.
* Personal use must not affect the internet service available to other users, for example high bandwidth downloads or streaming.
* All internet usage regardless of whether for company or personal use should be appropriate.
* Inappropriate use includes the viewing or downloading of inappropriate, illegal or offensive material or accessing material which may offend others in the vicinity.

# Internet Security

Used unwisely the internet can be a source of security problems that can do significant damage to the company’s reputation and data, personal data and customer data. Therefore:

* Users must not knowingly introduce any malware to the company and must not access or download files from an untrusted source.
* Users must not attempt to gain access to websites or resources that they are not authorised for, wither within or outside the business.
* Company data should only be uploaded or shared when authorised and via authorised routes (see Data Protection Policies).
* Users must not steal, use or disclose someone else’s login or password.

Staff must always consider the security of the company’s and individual’s data when using the internet.

# Inappropriate content

There are many sources of inappropriate content and materials available online. It is important for employees to understand that viewing or distributing inappropriate content is not acceptable under any circumstances.

Users must not:

* Take part in any activities on the internet that could bring the company into disrepute.
* Create or transmit material that might be defamatory or incur liability for the company. View, download, create or distribute any inappropriate content or material.

Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

This definition of inappropriate content or material also covers any 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.

* Use the internet for any illegal or criminal activities.
* Send offensive or harassing material to others.
* Broadcast unsolicited personal views on social, political, religious or other non-business-related matters.
* Send or post messages or material that could damage Retirement Capital’s image or reputation

# Copyright

Retirement Capital respects and operates within copyright laws. Users may not use the internet to:

* Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
* Download illegal copies of music, films, games or other software, whether via filesharing services or other technologies.

Employees must not use the company’s equipment, software or internet connection to perform any tasks which may involve breach of copyright law.

# Company Email

The Company recognises that email is a key communication tool. It encourages its employees to use email whenever appropriate.

For instance, staff members may use email to:

* Communicate with customers or suppliers
* Market the company’s products
* Distribute information to colleagues

The company also recognises that email is an important tool in many people’s daily lives. However, emails of a personal nature should be sent via personal and not company email accounts.

* Personal email use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.
* All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate, no matter whether it is being sent or received for business or personal reasons.
* Personal email use must not affect the email service available to other users. For instance, sending exceptionally large files by email could slow access for other employees.

Only people who have been authorised to use email at Retirement Capital may do so.

* Authorisation is usually provided by an employee’s line manager or the company IT department. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.
* Unauthorised use of the company’s email system is prohibited.
* Employees who use company email without authorisation — or who provide access to unauthorised people — may have disciplinary action taken against them.

# Email security

Used inappropriately, email can be a source of security problems for the company. Users of the company email system must not:

* Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.
* Disable security or email scanning software. These tools are essential to protect the business from security problems.
* Send confidential company data via email. The IT department can advise on appropriate tools to use instead.
* Access another user’s company email account. If they require access to a specific message (for instance, while an employee is off sick), they should approach their line manager or the IT department.

Staff members must always consider the security of the company’s systems and data when using email. If required, help and guidance is available from line managers.

Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception.

Although such interceptions are rare, it’s best to regard email as an open communication system, not suitable for confidential messages and information.

# Inappropriate email content and use

The company email system must not be used to send or store inappropriate content or materials.

It is important employees understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances.

Users must not:

* Write or send emails that might be defamatory or incur liability for the company.
* Create or distribute any inappropriate content or material via email.

Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

This definition of inappropriate content or material also covers any 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.

* Use email for any illegal or criminal activities.
* Send offensive or harassing emails to others.
* Send messages or material that could damage [company name]’s image or reputation.

Any user who receives an email they consider to be inappropriate should report this to their line manager or supervisor.

# Company Equipment

The Company provides equipment for the use of employees when engaging in the Company’s business. These devices have been set up according to the requirements of the Company’s security policies and obligations and must not be interfered with by:

* Deactivating any security application or software installed by the company
* Changing any security levels
* Installing additional software
* Changing any settings

All company owned equipment must be returned to the company at the end of employment of contract. No attempt to download or copy information on the equipment will be made.

# Portable data devices

From time to time it may be necessary to carry company or customer data on portable devices such as memory sticks or portable hard drives.

The use of such devices is only permitted when absolutely necessary and when the devices have been encrypted by a secure encryption service such as VeraCrypt.

# Monitoring

Company IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use. The company therefore reserves the right to monitor use of the internet, to examine systems and review the data stored in those systems. Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all internet data written, sent or received through the company’s computer systems is part of official Retirement Capital records. The company can be legally compelled to show that information to law enforcement agencies or other parties. Users should always ensure that the business information sent over or uploaded to the internet is accurate, appropriate, ethical, and legal.

Knowingly breaching this internet use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment. Employees, contractors and other users may also be held personally liable for violating this policy. Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

***Document Owner and Approval***

The Quality Manger is the owner of this document and is responsible for ensuring that this work instruction is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This work instruction was approved by the Chief Information Security Officer (CISO (DIRECTOR)) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |