REAL First Aid Ltd

IT & SOCIAL MEDIA POLICY

7th March 2023

1. E-mail and Internet Acceptable Use

Use of email and internet by employees and associates and associates of Real First Aid Ltd is permitted and encouraged where such use supports the goals and objectives of the business.

However, Real First Aid Ltd has a policy for the use of email whereby the employee must ensure that they:

- comply with current legislation
- use email and internet in an acceptable way
- do not create unnecessary business risk to the company by their misuse of email or internet

1.1 Unacceptable behaviour - Email

The following behaviour by an employee is considered unacceptable:

1.1.1 use of company communications systems to set up personal businesses or send chain letters

1.1.2 forwarding of confidential information to external locations

1.1.3 distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal

1.1.4 distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment

1.1.5 accessing copyrighted information in a way that violates the copyright

1.1.6 breaking into the company's or another organisation's system or unauthorised use of a password/mailbox

1.1.7 broadcasting unsolicited personal views on social, political, religious or other non-business related matters

1.1.8 transmitting unsolicited commercial or advertising material

1.1.9 undertaking deliberate activities that waste staff effort or networked resources

1.1.10 introducing any form of computer virus or malware into the corporate network

1.2 Unacceptable behaviour – Internet

1.2.1 visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material

1.2.2 using the computer to perpetrate any form of fraud, or software, film or music piracy

1.2.3 using the internet to send offensive or harassing material to other users

1.2.4 downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence

1.2.5 hacking into unauthorised areas

1.2.6 publishing defamatory and/or knowingly false material about [business name], your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format

1.2.7 revealing confidential information about [business name] in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions

1.2.8 undertaking deliberate activities that waste staff effort or networked resources

1.2.9 introducing any form of malicious software into the corporate network

1.3 Monitoring

All of the company's email resources are provided for business purposes. The company maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees and associates.

2. Social Media

Employees and associates should be aware of the effect their actions may have on their images, as well as company's image. The information that employees and associates post or publish may be public information for a long time.

Employees and associates should be aware that the company may observe content and information made available by employees and associates through social media. Employees and associates should use their best judgment in posting material that is neither inappropriate nor harmful to the company, its employees and associates, or customers.

2.1. Unacceptable use – Social Media

2.1.1. Posting on behalf or, or presenting views as the company.

2.1.2. Posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.

2.1.3. Publishing, posting or release any information that is considered confidential or not public. If there are questions about what is considered confidential - assume that it is.

2.1.4. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees and

associates should refer these inquiries to authorized the company spokespersons.

2.1.5. Referencing or posting images of current or former employees and associates, vendors or suppliers without permission.

2.1.6. The unauthorized use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

2.1.7. Computer systems are to be used for business purposes only. When using company's computer systems, use of social media for personal purposes is not permitted.

2.2. Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record. [These procedures will be specific to your business. They should reflect your normal operational and disciplinary processes. You should establish them from the outset and include them in your acceptable use policy.]

3. Laptop Security

If provided with a company laptop employees and associates shall exercise appropriate professional judgment and common sense when using them. All laptops, equipment and accessories are property of Real First Aid Ltd and are provided to employees and associates for a period of time as deemed appropriate by the company.

3.1. Responsibilities

3.1.1. As a condition of their use, employees and associates must comply with and agree to all of the following:

3.1.2. Prior to being issued a company laptop, employees and associates will sign the Laptop Acceptance Form and agree to all outlined policies.

3.1.3. Employees and associates should NOT attempt to install software or hardware or change the system configuration including network settings.

3.1.4. Employees and associates are expected to protect laptops, equipment and accessories from damage and theft.

3.1.5. Each associate is financially responsible for any hardware or software damage that occurs off-site and/or software damage.

3.1.6. Employees and associates will not be held responsible for computer problems resulting from regular work-related use; however, employees and associates

will be held personally responsible for any problems caused by their negligence as deemed by the company.

3.1.7. Employees and associates will provide access to any laptop computer or accessories they have been assigned upon BEHCON's request.

3.2. General Laptop Rules

You are responsible for protecting your laptop from loss or theft and for protecting the information it contains. These rules are provided to assist in assuring that your laptop is secure at all times. Not all conceivable situations can be covered in this document.

Employees and associates must realize that common sense should be your guide when faced with unusual or unforeseen situations.

3.2.1. Power off your laptop whenever it is not in use. Do not carry the laptop in suspend or hibernation mode.

3.2.2. Use laptop lock-down cable systems whenever possible.

3.2.3. Personal use of the laptop, equipment and accessories is prohibited

3.2.4. Keep your laptop close to you and in sight. Otherwise, keep it locked away securely.

3.2.5. Never store passwords with your laptop or in its carrying case.

3.2.6. Other forms of user authentication should be kept separate from your laptop at all times.

3.2.7. Do not travel without your laptop if it is not needed.

3.2.8. Make sure that your hands are clean before using them. Hand lotion is a contributing factor to dirt and dust, please make sure your hands are free from lotion before using the computer. It is costly to change a laptop keyboard and/or touchpad that has been damaged be excessive dirt.

3.2.9. Do not place drinks or food in close proximity to your laptop.

3.3. While at the Office

3.3.1. When away from your desk, leave your laptop in locked / "log in required" protection status.

3.3.2. Laptops should be taken home at night or secured out of sight in a locked drawer, cabinet, or locked overhead compartment of your desk.

3.3.3. Make sure that the laptop is in locked / "log in required" status if you need to walk away from your laptop.

3.3.4. Do not leave your laptop unattended if you leave the meeting room. Ensure that someone is designated to remain in the room with any laptops, or that the laptops are secured to immovable objects, or that the meeting room door is

locked.

3.4. While Traveling In a Personal or Rental Car

3.4.1. Extreme temperatures can damage a laptop. You should not leave a laptop in an unattended vehicle.

3.4.2. If you must leave you're your laptop in an unattended vehicle for a short period of time, always lock your laptop in the boot of the car. A visible laptop is a target.

3.5. In Hotels

3.5.1. Never leave your laptop unattended in hotel rooms.

3.5.2. If you leave your room for any period of time, secure your laptop in the room safe. If a room safe is too small or unavailable, lock your laptop in your travel luggage.

3.5.3. Always attempt to keep evidence that you may be traveling with a laptop out of site.

3.5.4. Store the carry case and peripherals, such as a mouse and a charger, in your travel luggage.

3.6. While Traveling by Air

3.6.1. Check with your airline to verify whether laptops can be carried on the plane.

3.6.2. Always carry your laptop with you; only place your laptop in checked baggage if required by the airline or airport security.

3.6.3. If required by airport authorities, employees and associates may place electronic communication devices and encrypted laptops in their checked luggage.

3.6.4. All devices must be powered off before they are packed.

3.6.5. Remove the battery from laptops.

3.6.6. Wrap your laptop in clothing to protect it.

3.6.7. If possible, pack your laptop in luggage rather than your briefcase. This will make it less conspicuous to thieves.

3.6.8. Lock all luggage and briefcase compartments with a lock approved by the Transportation Safety Administration (TSA).

3.6.9. Beware of staged delays at security checkpoints; many thieves use this tactic to steal laptops.

3.6.10. Do not send your laptop through the screening devices until you are about to pass through the checkpoint. Keep your laptop close to you at all times. If an overhead compartment within an unobstructed view is not available, consider placing your laptop underneath the seat in front of you.

4. Passwords

Employees and associates must access a variety of IT resources, including computers and other hardware devices, data storage systems, and on-line accounts. Passwords are a key part of our strategy to make sure only authorized people can access those resources and data.

4.1. All employees and associates who have access to any of those resources are responsible for:

- Implementing passwords given to you by the company
- choosing strong passwords when using your own passwords
- protecting their log-in information from unauthorized people.

4.2. Dictated Passwords

All of our systems and on-line accounts have unique passwords. Under no circumstances should an employee or associate change a company password without permission from the Director.

4.3. Password creation

4.3.1. All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters.

4.3.2. In addition to meeting those requirements, employees and associates should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective.

4.3.3. A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided.

4.3.4. Our recommended format is that a unique stub, related to the system or account in question, precedes a common password element to allow unique passwords to be created for each account or system without have to remember entirely unique combinations such as [Unique stub][random word][year][special character].

For example, if your basic password is “Rainbow” your password for email in 2018 could be “EmailRainbow18&”

4.3.5. Employees must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.

4.3.6. All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question.

4.3.7. If the security of a password is in doubt, for example, if it appears that an unauthorized person has logged in to the account, the password must be changed immediately.

4.3.8. Default passwords, such as those created for new employees or associates when they start, must be changed as quickly as possible.

4.4. Protecting passwords

4.4.1. Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

4.4.2. Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

4.4.3. Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.

4.4.4. Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

4.4.5. Employees may not use password managers or other tools to help store and remember passwords without permission.

5. Remote Access and Mobile Computing

5.1. Purpose

The purpose of this policy is to define standards and restrictions for connecting to

The company's internal network from an external location via remote access technology. The company's resources (i.e. corporate data, computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image.

All remote access for employees and associates must be achieved with minimum risk to the company via standard, audited methods.

5.2. Context

Company-based systems have until recently been inaccessible from outside the business premises. A remote access solution offers several benefits including what can be accessed, from where it can be accessed and when.

5.3. Remote Access

Remote access is defined as any connection to the company's resources from any off-site locations.

5.4. Scope

5.4.1. This policy applies to all authorised employees and associates who remotely access the company's data and networks.

5.4.2. Employees and associates of the company are not automatically granted the privileges of remote access privileges.

5.4.3. Any and all work performed for the company through a remote access connection is covered by this policy.

5.4.4. Work can include (but is not limited to) e-mail correspondence, web browsing, accessing server-stored files, and any other company application.

5.5. Supported Technology

5.5.1. All remote access connections will be centrally managed by the company by encryption and strong password protection.

5.5.2. Remote access connections as defined by this policy mean Virtual Private Network (VPN) connections which establish a secure towards the company's network over home Broadband, or via WiFi connections in public places.

5.5.3. These VPN connections will be made via NordVPN client ONLY.

5.6. System Requirements

5.6.1. Any member of staff wishing to access company resources via a VPN connection must be able to satisfy ICT Services that they have a PC or laptop with Windows XP or newer (including the latest Windows updates), or a MAC with at least MAC OSX

5.6.2. Any connection depends on the user having an active Internet connection.

5.7. Procedures

5.7.1. It is the responsibility of any employee or associate of the company with remote access privileges to ensure that their VPN connection remains as secure as his or her network access within the office.

5.7.2. It is imperative that any VPN connection used to conduct company business be utilized appropriately, responsibly, and ethically.

5.7.3. Therefore, the following rules must be observed:

5.7.3.1. General access to the Internet from home is permitted although this must not be used for recreational purposes – the remote access connection must be disconnected prior to accessing such Internet sites.

5.7.3.2. Employees and associates must maintain their personal Windows or Mac operating system with current updates to avoid security issues.

5.7.3.3. Employees must not disclose their passwords to anyone, including family members if business work is conducted from home.

5.7.3.4. All remote computer equipment and devices used for business work, whether personal- or college owned must have installed whatever antivirus software is deemed necessary and appropriate by the company.

5.7.3.5. Remote users using public areas for wireless Internet access must use a Cisco

5.7.3.6. WiFi users must disconnect wireless sessions when not in use in order to mitigate attacks by hackers and eavesdroppers.

5.7.3.7. In order to avoid confusing official company business with personal communications, employees and associates with remote access privileges and dedicates email addresses must never use personal e-mail accounts (eg. Hotmail, Yahoo, etc.) to conduct company business.

6. Declaration

On behalf of **Real First Aid Ltd** we, the undersigned, will oversee the implementation of the IT & Social Media Policy and take all necessary steps to ensure it is adhered to.

Signed: 

(n.b. One of the signatories should be the Director)

Name:	**Adam Gent**
Position within the Company:	**Director**
Date:	**7th March 2023**