Acceptable Use Policy

Table of Contents

Introduction

Louise White MamaActive and Buggyfit Instructor (known as Louise White in these documents) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to established culture of openness, trust and integrity. We are committed to protecting employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing, and FTP, are the property of Louise White MamaActive/ Buggyfit. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Louise White MamaActive/ Buggyfit employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Policy Details

Policy Number: 2001_USAGE

Policy Date: 25th May 2018

Purpose of the Policy

The purpose of this policy is to outline the acceptable use of computer equipment at Louise White MamaActive/ Buggyfit. These rules are in place to protect the employee and Louise White MamaActive/ Buggyfit. Inappropriate use exposes Louise White MamaActive/Buggyfit to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Louise White MamaActive/Buggyfit business or interact with internal networks and business systems, whether owned or leased by Louise White MamaActive/Buggyfit, the employee, Trainer, instructor or a third party. All employees, contractors, consultants, temporary, and other workers at Louise White MamaActive/Buggyfit and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Louise White MamaActive/Buggyfit policies and standards, and local laws and regulation.

This policy applies to employees, licensees, contractors, consultants, trainers, instructors, temporaries, and other workers at Louise White MamaActive/Buggyfit. , including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Louise White MamaActive/Buggyfit.

Policy

General Use and Ownership

Louise White MamaActive/Buggyfit proprietary information stored on electronic and computing devices whether owned or leased by Louise White MamaActive/Buggyfit. The employee or a third party remains the sole property of Louise White MamaActive/Buggyfit. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Louise White MamaActive/Buggyfit proprietary information.

You may access, use or share Louise White MamaActive/Buggyfit proprietary information only to the extent it is authorised and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individuals are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by company policies on personal use, and if there is any uncertainty, employees should consult management.

For security and network maintenance purposes, authorised individuals within Louise White MamaActive/Buggyfit. may monitor equipment, systems and network traffic at any time.

 Louise White MamaActive/Buggyfit reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with the Remote Access Policy.

System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Postings by employees from a email address to newsgroups Louise White MamaActive/Buggyfit should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Louise White MamaActive/Buggyfit unless posting is in the course of business duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Louise White MamaActive/Buggyfit authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Louise White MamaActive/Buggy fit's owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Louise White MamaActive/Buggyfit.

- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Louise White MamaActive/Buggyfit. or the end user does not have an active license is strictly prohibited.

- Accessing data, a server or an account for any purpose other than conducting Louise White MamaActive/Buggyfit business, even if you have authorised access, is prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Using a Louise White MamaActive/Buggyfit computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers of products, items, or services originating from any Louise White MamaActive/Buggyfit account.

- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to TTSD is made.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.

- Introducing honey pots, honey nets, or similar technology on the Louise White MamaActive/Buggyfit network.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

- Providing information about, or lists of, Louise White MamaActive/Buggyfit employees to parties outside Louise White MamaActive/Buggyfit.

Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to management.

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

- Unauthorised use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

- Creating or forwarding "chain letters "or other "pyramid" schemes of any type.

- Use of unsolicited email originating from within Louise White MamaActive/Buggy fit's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Louise White MamaActive/Buggyfit or connected via Louise White MamaActive/Buggyfit's network.

- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Policy Compliance

Compliance Measurement

Current Partners of the business will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Louise White

Non-Compliance

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

Additional Policies

Remote Access Policy

Password Policy

Confidential Information Policy

Policy Review

This policy will be reviewed on an Annual basis, starting from the 25th May 2019. Any changes will be documented, communicated to the relevant parties and copies held on file at our offices.

Last Review Date: _____

Next Review Date: _____

Policy Authorised by: _____

Signature: _____

Date: _____