1. Overview

Mars Institute (MARS) is committed to protecting their Employees, Staff, Trainers, Contractors and Students from illegal or damaging actions by individuals, either knowingly or unknowingly. It is expected that Students demonstrate respect, integrity, responsibility and honesty in communications and actions at all times in their use of Information and Communication Technology (ICT).

Students have the right to learn in a safe environment, including when they have access to ICT to enhance their learning. MARS is committed to the responsible and educational use of ICT and to providing secure access to these services as part of the Student and Staff learning and teaching experience. MARS supplied devices and personal devices are all expected to be used in accordance with this Policy to enhance learning and teaching and support positive wellbeing practices.

ICT, including but not limited to computer equipment, software, operating systems, file storage media, communication technology and Internet Access, are the property of MARS. These systems are to be used for training and research purposes as well as limited personal training related communications.

Effective security is a team effort involving the participation and support of every MARS Employee, Staff, Trainers, Contractors and Students and visitors who utilise the facilities in our training centres. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This Policy applies to all Employees, Staff, Trainers, Contractors and Students and visitors who use MARS owned resources such as Computer Networks (including Internet services), Personal Computers, Loan Laptops, iPad, Tablets and Printers/Photocopiers. (but not limited to). MARS reserves the right to monitor all computer related activity and to assist authorities to our fullest extent should a breach of law occur.

ICT includes any electronic device or application used to communicate, create, disseminate, store or manage information such as text, images, audio or video. Personal devices include (but is not limited to) mobile phones, smart watches, iPads and other tablet computers, dedicated games consoles and any other internet connected devices.

2. Purpose

The purpose of this Policy is to outline the acceptable use of ICT equipment at MARS. These rules are in place to protect the equipment from damage due to Viruses and malware, or misuse, and to ensure that equipment is in good working order suitable for use by all Students. Additionally, the Policy's purpose is to provide a set of guidelines to reduce the risk of other Students and Staff exposure to inappropriate Internet content, including Social Media content.

'Social Media' refers to a range of online platforms and applications – such as social networking sites, wikis, blogs, microblogs, video and audio sharing sites, and message boards – that allow people to easily publish, share and discuss content. This includes any department enterprise social media platforms, such as Yammer, Tic Toc, Facebook, Twitter and Instagram and Google Classroom.

This Policy outlines:

- The standard of online behaviour to promote a safe online environment for the MARS Students and Staff
- The rights and responsibilities of Students; and
- Possible consequences if this Policy is breached.

3. Policy

The Policy items listed below provide guidelines for activities which fall into the category of unacceptable use in MARS.

MARS Owned Resources:

Under no circumstances is a Student, Employee or Staff member to engage in any activity that is illegal under local, state, federal or law while utilising MARS owned resources.

The following activities are, in general, *Prohibited*:

1) Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources such as copyrighted music or movies.

2) Installation of any software on desktop or laptop computers.

3) Storage of personal files on computers. This includes personal photos and music files.
4) Intentional introduction of malicious programs into the network (e.g., viruses, worms, Trojan horses, etc.).
5) Use of MARS computing assets 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.
6) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Student, Employee or Trainer is not an intended recipient, or logging into a device, server or account that the Student is not expressly authorised to access.
7) Circumventing user authentication or security of any Information Technology device, network or account.
8) Using a login account that is allocated to another Student or Staff Member.
9) Any form of harassment via email, telephone, social media or messaging, whether through language, frequency, or size of messages.
10) Video or Audio recording of training sessions, or the Trainer, or Students in the classroom without prior permission from the Training Manager/ CEO.
11) Using images of MARS Staff, Students or images relating to MARS's facilities without permission from the Training Manager/ CEO.
12) Communicating on behalf of MARS without permission from the Training Manager/ CEO;
13) Any online activity such as denigrating MARS through criticism of MARS's policies, practices or personnel resulting in bringing MARS into disrepute.
14) Removal of, tampering with, or damage to, any Information Technology hardware such as (but not limited to) Computer Mice, Keyboards, Screens, PCs, Printers, Projectors, Memory devices, Networking equipment, cameras, Tablets, iPads or cables.
15) Abuse of download limitations by excessive downloading of large files for personal use or continuous streaming of media from internet sources such as Internet Radio Stations.
16) Student use of Social Networking sites such as Facebook, Snapchat, Instagram and Kik whilst at MARS is forbidden. MARS's ICT resources are provided for teaching and learning.
17) Accessing or attempting to access inappropriate or blocked internet sites.
18) Creation or forwarding of texts, posts, messages or images that may be illegal, offensive, intimidating, defamatory, sexually explicit or aggressive

Staff, Contractor, and Students owned resources:

The following activities are, in general, *Prohibited*:

1) Creation or forwarding of texts, posts, messages or images that may be illegal, offensive, intimidating, defamatory, sexually explicit or aggressive through MARS platforms
2) Abuse of download limitations by excessive downloading of large files for personal use or continuous streaming of media from internet sources such as Internet Radio Stations, while using MARS internet/data
3) Communicating on behalf of MARS without permission from the Training Manager/ CEO;
4) Using images of MARS Staff, Students or images relating to MARS's facilities without permission from the Training Manager/ CEO.
5) Using a login account that is allocated to another Student or Staff Member.
6) Any form of harassment via email, telephone, social media or messaging, whether through language, frequency, or size of messages.
7) Video or Audio recording of training sessions, or the Trainer, or Students in the classroom without prior permission from the Training Manager/ CEO.
8) Intentional introduction of malicious programs into the network (e.g., viruses, worms, Trojan horses, etc.).
9) Unauthorised copying of MARS materials, resources and student/staff personal information.

4. Online Learning Environment

TOC provides Students, Staff and Trainers, Contractors with access to online learning resources via the Internet and Learning Management System (LMS). In some instances, personal devices such as iPads/Tablets/Loan Laptops are provided to Students to enhance their learning experience.

It is the Student's, Staff, Trainer's or Contractors responsibility to ensure that portable devices assigned to them, such as iPads/Tablets/Laptops, are not damaged, lost or stolen. Any incidents relating to mistreatment of portable devices must be reported to MARS Staff immediately.

Students, Staff and Trainers, Contractors must secure their logins to learning systems with strong passwords and not share password information with other Students/, Staff, Trainers or Contractors.

5. Enforcement

It is the responsibility of the person who witnesses or suspects a breach of this Policy or experiences a breach of this Policy to report it immediately. Any breach will be investigated and considered by the Training Manager/ CEO. Each breach will be dealt with on a case-by-case basis.

Sanctions for breach by a student may include:

1) Providing a warning, counselling, withdrawal of certain privileges or opportunities, suspension, expulsion, refusal to re-enrol the student, civil or criminal prosecution under applicable laws.

2) Sanctions for breach by a Staff member, Employee, Contractor, or Visitor may include:

3) Providing a warning, counselling, withdrawal of certain privileges or opportunities, suspension from duties, termination of employment, civil or criminal prosecution under applicable laws.

Note that any offence associated with any security breach, pornography or insulting behaviour will be automatically classified as being of a serious nature for Academic Misconduct.

Records of reported incidents of ICT misuse are maintained and analysed in order to identify persistent offenders and to implement targeted prevention strategies where appropriate.

MARS reserves the right to request that certain subjects are avoided, defamatory posts are withdrawn, and inappropriate or offensive comments or images removed. MARS has the right to monitor on an intermittent or continuous basis the information input or output, or other use of the network and any device attached to the network, including the sending and receipt of emails and the accessing of Internet sites, and to check any material put on the network and in personal user accounts or on MARS owned devices, in order to determine whether it is suitable for use in learning and complies with this Policy. This includes files saved to personal network space and the content of emails.

Privacy will be respected when accounts are monitored.