GENERAL DOCUMENT INFORMATION				
1	**Document category**	Policy		
2	**Document approver**	Data & Information Management Department Head		
3	**Minimum list of document users to be notified upon release of document update**	All Staff and Students		
4	**Document change history**			
	B	**DCN #**	**Date released**	**Change originator**
		051/2014	8th August 2014	Pace Mario
		Change history (Section/change details)		
		Transferred Policy to MCAST Corporate template and released as an approved document.		
	C	**DCN #**	**Date released**	**Change originator**
		Change history (Section/change details)		

PLEASE READ BELOW BEFORE REFERRING TO THIS DOCUMENT

Instructions for document users with access to College SharePoint System

All MCAST employees can access current, controlled and approved documents related to the Quality Management System from the College SharePoint system URL http://eportal.mcast.edu.mt/Main/Pages/DocumetControl.

*Document users who do have access to SharePoint are therefore encouraged **NOT** to retain printed hard copies of the Quality Management System documents.*

If however a hard copy of the document is required, the user is to ensure that the printed document is the current revision.

Continuous Improvement

*Procedures are meant to be 'living' documents that need to be followed, implemented and maintained. If the procedure does not reflect the current, correct work practice, it needs to be updated! Contact your Document Controller on Ext 7121 **today**. !*

CONTENTS

SECTION 1 : MCAST IT POLICY

1.1) Scope of Policy

This policy is relevant to MCAST students, staff, and all individuals or entities using any of the MCAST IT Resources and all uses of such IT Resources.

1.2) Purpose for Policy

The purpose of this policy is to describe the appropriate use of MCAST IT facilities, associated responsibilities, and rights of all Users of the College's IT Facilities and Official MCAST E-mail Accounts.

1.3) Statement of Policy

MCAST provides some, if not all, users with electronic access, consisting of an email system, a network connection, and Internet/Intranet access. This policy governs all use of the College's network, Internet/Intranet access and email system at all the College's locations and offices.

Any User of MCAST IT resources consents to all provisions of this policy and agrees to comply with all of the terms and conditions set forth herein, all other applicable MCAST policies, regulations, and procedures.

Users of MCAST IT facilities, whose actions violate this policy or any other MCAST policy/ regulation or national legislation may be subject to revocation or limitation of electronic access privileges as well as other disciplinary actions or may be referred to appropriate external authorities

SECTION 2 : MCAST E-MAIL POLICY

2.1) Access to E-mail:

MCAST provides E-mail Facilities for legitimate College-related activities to faculty, students, staff, and other individuals and entities granted e-mail privileges at MCAST, as well as connections between on-campus electronic mail systems and external data networks. The use of MCAST E-mail Facilities -- like the use of any other MCAST-provided resource and like any other College-related activity -- is subject to the normal requirements of legal and ethical behaviour within the MCAST. Thus, legitimate use of MCAST E-mail Facilities does not extend to whatever is technically possible.

2.2) MCAST E-mail Account:

MCAST is the owner of centralized e-mail and directory information for the whole college, and provides creation, management, and distribution of Official MCAST E-mail Accounts.

Staff members with access to an MCAST-owned computer on campus, students, and faculty are required to activate their Official MCAST E-mail Account. Users are expected to read, and shall be presumed to have received and read, all official MCAST e-mail messages sent to their Official MCAST E-mail Accounts.

Users may forward their MCAST e-mail to another e-mail address, but any User who does so expressly assumes all responsibility for delivery beyond the @mcast.edu.mt domain.

2.3) E-mail Acceptable Use:

MCAST provides E-mail & Collaboration Facilities for activities and associated administrative functions supporting its mission to provide universally accessible vocational and professional education and training with an international dimension, responsive to the needs of the individual and the economy. Although modest personal use of College E-mail Facilities is allowed, College E-mail Facilities should be used for College-related educational and administrative purposes. Any use of MCAST E-mail Facilities that interferes with the College activities and functions or does not respect the image and reputation of MCAST is improper.

Policies and regulations that apply to other forms of communications at the MCAST also apply to electronic mail.

In addition, the following specific actions and uses of MCAST E-mail Facilities are improper:

1. Concealment or misrepresentation of names or affiliations in e-mail messages.
2. Alteration of source or destination address of e-mail.
3. Use of e-mail for commercial or private business purposes that have not been approved by MCAST.
4. Use of e-mail for organized political activity or political solicitation.
5. Use of e-mail to harass or threaten other individuals.
6. Use of e-mail that degrades or demeans other individuals.

2.4) Public Record and Privacy:

MCAST does not monitor the content of electronic mail as a routine procedure. MCAST reserves the right to inspect, copy, store, or disclose the contents of electronic mail messages, but will do so only when it believes these actions are appropriate to: prevent or correct improper use of College E-Mail Facilities; ensure compliance with MCAST policies, procedures, or regulations; satisfy a legal obligation; or ensure the proper operations of College E-mail facilities or any of the MCAST Data Network. Whenever MCAST believes such actions are necessary must first obtain the written approval of the Chief Administration Office or the Chief Executive Officer.

2.5) Use of E-mail for MCAST Matters:

The Official MCAST E-mail Account shall be considered an official means for communicating any MCAST matters, and may in some cases be the sole means of communication. Users are expected to read, and shall be presumed to have received and read, all official MCAST e-mail messages sent to their Official MCAST E-mail Accounts. Because the contents of such e-mail are subject to laws governing public records, users will need to exercise judgment in sending content that may be deemed confidential. Furthermore, e-mail transmissions may not be secure, and contents that are expected to remain confidential should not be communicated via e-mail.

Directors and their appointees may send Broad-Based Messages relating to MCAST matters without any prior approval. The author of any of these messages, however, assumes responsibility for assuring that messages do not violate any MCAST policies, regulations, or procedures. Disclaimers of confidentiality included in e-mail messages do not protect the sender if confidential information is shared or disclosed inappropriately.

2.6) E-Mail Retention and Disposal:

Mailboxes will be deleted after two weeks from termination of employment/enrolment unless otherwise instructed.

2.7) Disclaimer

MCAST makes no warranties of any kind, whether expressed or implied, with respect to the College E-mail Facilities it provides. The College will not be responsible for damages resulting from the use of

MCAST E-mail Facilities, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a College user, or by the User's error or omissions. The College specifically denies any responsibility for the accuracy or quality of information obtained through MCAST E-mail Facilities, except material represented as an official College record.

2.8) Official MCAST E-mail Account

An Official MCAST E-mail Account of the form name.surname@mcast.edu.mt is provided to faculty, students, staff, and other individuals and entities granted e-mail privileges at MCAST. It is automatically created for admitted and enrolled students as well as actively employed faculty/staff.

SECTION 3 : MCAST NETWORK AND INTERNET POLICY

3.1) Personal responsibility

By accepting an account password, related information, and accessing the College's network or internet system a user agrees to adhere to the College policies regarding their use. The user also agrees to report any misuse or policy violations to his/her direct superior.

3.2) Permitted use and term

Use of the network and the internet is a privilege, not a right. Use of network and internet access extends throughout a user's term of employment/enrolment, providing the user does not violate the College's policies regarding network, internet or intranet use.

3.3) Availability and access

The College reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security or other concerns.

3.4) Content and communications

The college, at its own discretion, will determine what materials, files, information, software, communications, and other content and all activity will be permitted or prohibited.

3.5) Privacy

Network and internet access is provided as a tool for College matters. The College reserves the right to monitor, inspect, copy, review and store at any time, without prior notice, and all usage of the network and internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of MCAST. A user should have no expectation of privacy regarding them. Network administrators may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring users are using the system consistently with this policy.

3.6) Downloaded files

Any files authorized for download from the internet must be scanned with virus detection software before being accessed. Users are reminded that information obtained from the internet is not always reliable and should be verified for accuracy before use.

3.7) Confidential information

With the approval of management, users may use email to communicate confidential information internally to those with a need to know. Such emails must be marked confidential. For purposes of this policy confidential information includes, but is not limited to:

1. Procedures for computer access and passwords of the college's users, program manuals, user manuals or other documentation, run books, screen, file, or database layouts, system flowcharts, and documentation normally related to the design and implementation of any computer programs delivered by the College relating to computer programs or systems installed for internal use.
2. Any other information relating to the college's research, development, inventions and purchasing.

3.8) Prohibited activities

Users are prohibited from using the college's email system, network, or internet/intranet access for the following activities:

1. Printing or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright laws.
2. Using software that is not licensed by the manufacturer or approved by the college.
3. Sending, printing or otherwise disseminating the college's proprietary data, or any other information deemed confidential by the college, to unauthorized persons.
4. Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment.
5. Making offensive or harassing statements based on race, colour, religion, national origin, veteran status, disability, age, sex, or sexual orientation.
6. Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements.
7. A user should notify their direct superior immediately upon receiving such a message. This type of message should not be forwarded.
8. Sending or forwarding a message that discloses personal information without college's authorization. This shall also include assessing, transmitting, receiving, or seeking confidential information about fellow users without authorization.
9. Sending ethnic, sexual preference or gender-related slurs and/or jokes via e-mail. "Jokes", which often contain objectionable material, are easily misconstrued when communicated electronically.
10. Sending or soliciting sexually oriented images or messages.
11. Attempting to access or visit sites featuring pornography, terrorism, espionage, theft and drugs.
12. Gambling or engaging in any other criminal activity in violation of National Law.
13. Engaging in unethical activities or content.
14. Participating in activities, including the preparation of dissemination of content, which could damage the college's professional image and reputation.
15. Permitting or granting use of an email or system account to another user or persons outside the college. Permitting another person to use an account or password to access the network or the internet, including, but not limited to, someone whose access has been denied or terminated, is a violation of this policy.
16. Using another user's password or impersonating another person while communicating or assessing the network or internet.
17. Introducing a virus, harmful component, corrupted data or the malicious tampering with any of the college's computer systems.
18. Connecting personal equipment to MCAST network without the prior authorization of the IT department is a violation of this policy. Any user failing to comply with this rule will be subject to disciplinary actions, up to and including termination of service. Moreover MCAST cannot be held responsible for any faults which may occur on personal equipment, even those resulting from force majeure. MCAST IT staff reserve the right to refuse to work/troubleshoot/install software or patches on any personal equipment brought by any user nor they can be held

responsible for any damages resulting from their intervention. Furthermore MCAST IT Staff reserve the right to disconnect any personal equipment which is connected to the MCAST network.

19. Personal equipment can only be connected to the Wifi network, and any person doing so must comply with MCAST's Wifi policy regulations.

3.9) Computer Equipment

The following policies are designed to reduce repair costs, maintain the integrity of our system and protect the college's assets. Users should adhere to the following:

1. Do not keep liquids or magnets on or near any computer equipment.
2. Do not remove any IT related equipment from the building without any written permission from your direct superior.
3. Do not transport disks, back and forth between home and office. This will help minimize exposure to viruses.

3.10) Compliance

Though each individual is responsible for his/her own actions, management personnel are responsible for ensuring user compliance with college policy. Any user aware of a policy violation should immediately report the violation to their direct superior. Users who violate this policy and/or use the college's email system, network, internet or intranet access for improper purposes will be subject to disciplinary actions, up to and including termination. (For the purpose of this clause students are to report to the respective director/deputy director of Institute)

3.11) Non compliance

Violation of these policies will result in disciplinary action up to and including termination of services.

SECTION 4 : SOFTWARE USAGE POLICIES AND PROCEDURES

4.1) Software Usage Policy- Statement

Software piracy is both a crime and a violation of the college software usage policy.
Users are to use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (Except for backup and archiving purposes by designated managerial personnel) is a violation of copyright law. In addition to being in violation of the law, unauthorized duplication of software is contrary to the college's standards of user conduct.

4.2) Compliance

To ensure compliance with software license agreements and the college's software usage policy, users must adhere to the following:

1. Users must use software in accordance with the manufacturer's license agreement and the college's software usage policy. The college licenses the use of computer software from a variety of outside companies. The college does not own the copyright to software licensed from other companies. Users acknowledge they do not own software or its related documentation. Users may not make additional copies of software, unless expressly authorized by the software publisher. The only expectation will be a single copy, as authorized by designated managerial personnel, for backup or archiving purposes.

2. The college prohibits the unauthorized duplication of software. Users illegally reproducing software will be subject to disciplinary actions. In addition, users illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.
3. Any user who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to the college, or who places or uses unauthorized software on the college's premises or equipment shall be subject to disciplinary actions, up to and including termination.
4. Users are not permitted to install their personal software into the college's computer system. Users are not permitted to copy software from the college's computer system for installation on home or other computers without authorization.
5. Any user issued additional copy or copies of software for home use acknowledges that such additional copies or license purchased for home use are the property of the college.
6. Users are prohibited from giving software to any other person not in the employ of the college. Under no circumstances will the college use software from an unauthorized source including but not limited to, the internet, home, friends or colleagues.
7. Users who suspect or become aware of software misuse are required to notify their direct superior.
8. All software used on college owned computers will be purchased through appropriate procedures. Consult your direct superior for proper procedures.

SECTION 5 : MCAST IT SECURITY POLICY

5.1) User Responsibilities

If a computer is assigned to a member of staff he/she shall act as custodian of that computer.
Each user is responsible for the security of all data held by him/her. All users must acknowledge in writing, prior to being granted access to computing facilities that they have read, understood and will comply with the MCAST IT Policy contained within this document, and that they are aware of the consequences of violating these policies and standards. These consequences include disciplinary action up to and including termination of employment, and in some cases include additional legal consequences.

It is the custodian's responsibility to ensure that any member of staff he/she authorizes to use his/her Computer has complied with the requirements of the previous paragraph. In addition, users are responsible for informing management of any actual or potential variances from security policies, standard and practices.

All data whether or not created by the user, stored on the computer and IT systems provided by the college, including backup copies cannot be considered to be the property of user. MCAST shall have unencumbered access to such content, subject to third party ownership rights.

5.2) Authentication

In order to maintain the confidentiality of the college's and user data held on computers, it is essential that only authorized users have access to the machines and to the data stored on them. A breach of confidentiality could lead to legal action or serious embarrassment to the college and/or the users should take all possible measures to ensure data is secure. This can be achieved by making use of the password facilities of the machine and software packages.

5.3) Access Control

To access the MCAST Network a user must have a login name and password. The login name is provided by the IT department together with an initial password, which must be changed immediately by the user. Only IT Staff may reactivate locked user accounts.

5.4) Unattended Computers

Computers should not be left unattended for a protracted period (e.g more than half an hour). In this case the computer should be switched off or locked.

5.5) Confidential Information on Computers

Confidential information may be stored on the computer's Hard Disk. The user is responsible that only authorized personnel see the information. Users are fully responsible for any confidential data stored in their computer.

Information held in MCAST computers is considered as confidential as outlined above. Users who replicate copies of any data on their laptop computers should ensure that they act in accordance with the policy defined by this document.

5.6) Data Integrity

Data stored on a computer may be lost in a number of ways, computers may be lost or stolen or may be accidentally damaged, data may be erased accidentally or corrupted due to hardware failure or Virus attacks. It is the user's responsibility to make sure that the data stored on his/her computer is backed up. Only in this matter can full recovery of data be ensured.

5.7) Backups

All users should ensure that they maintain up to date backups of all data under their control. This includes all data stored on their PC's hard disk. Data stored on MCAST's servers is regularly backed up by the IT Dept under the responsibility of the IT Manager.

5.8) Virus Detection and Cleansing

A user is responsible for ensuring that his/her college computer is equipped with the latest version of the college's virus checking software (updates are frequently released over the Network). Users must NEVER alter or stop this update operation.

This virus checker installed on all computers must be executed any time a user suspects that his/her computer has been exposed to a virus source.

Data originating from an infected computer should never be transported off the computer either by movable media, over the network or by e-mail. Deliberately spreading infected files is considered as an extremely serious offence.

5.9) Physical Security

Computers, in particular portable computers, are prone to theft. This is costly and potentially damaging in respect of the confidential data that may be held on the computers, together with other important documents. Although it is impossible to complete guard against theft, it is important that all necessary measures are taken and users take responsibility for equipment assigned to them.

Users are responsible for the physical protection of their computer and any other peripheral or backup media in their possession.

5.10) Hardware Protection

Users must ensure that their laptop provided by the college are stored safely when not in use. If laptops which are provided by the college are left in the office, they should be stored in a locked cabinet.

Laptops should not be left unattended in a vehicle, If this cannot be avoided it should be place out of site. E.g. luggage boot. Staff should never leave laptops in their vehicles in extreme climatic conditions, cold or heat, as this could damage the laptop.

Laptops must never be left unattended while travelling on public transport.

SECTION 6 : ELECTRONIC ACCESS POLICY

6.1) Acknowledgement of Receipt and Understanding

I hereby certify that I have read and fully understand the contents of the MCAST IT policy, furthermore, I have been given the opportunity to discuss any information contained therein or any concerns that I may have. I understand that my employment/enrolment and continued employment/enrolment is based in part upon my willingness to abide by and follow the college's policies, rules, regulations and procedures. I acknowledge that the college reserves the right to modify or amend its policies at any time without prior notice. These policies do not create any promises or contractual obligations between the college and its users. My signature below certifies my knowledge, acceptance and adherence to the college's policies, rules, regulations and procedures regarding electronic access.

SIGNATURE: _____

NAME & SURNAME _____

ID CARD NUMBER: | | | | | | | | | |

DATE: | | | | | | |

APPENDIX I - DEFINITIONS/GLOSSARY

Users : Any person using MCAST IT facilities/resources

College : MCAST – The Malta College of Arts Science & Technology.

Management ; Principal & CEO, MCAST Directors, Deputy Directors & Managers.

Network ; A group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or as many as thousands of users

Intranet ; An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.

Internet ; the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP

Email ; Short for ELECTRONIC MAIL, the transmission of messages over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, minicomputers, and computer networks have an e-mail system. Some electronic-mail systems are confined to a single computer system or network, but others have gateways to other computer systems, enabling users to send electronic mail anywhere in the world.