

| | | | | |
|------------------------|---------------------|--------------------------|---|------------------------------|
| Document Title | Wi-Fi POLICY | | | Page 1 of 5 |
| Document Number | 182 | Document Revision | A | Date Issued 8/8/14 |

| GENERAL INFORMATION | | | | |
|--|--|--|-----------------------------|--------------------------|
| 1 | Document type | 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 | | | |
| | A | DCTN # | Date released | Change originator |
| | | 52/2014 | 8 th August 2014 | Pace Mario |
| | | Change history (Section/change details) | | |
| | New procedure | | | |
| | | 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**. !

| | | | | |
|------------------------|---------------------|--------------------------|---|------------------------------|
| Document Title | Wi-Fi POLICY | | | Page 2 of 5 |
| Document Number | 182 | Document Revision | A | Date Issued 8/8/14 |

Contents

INTRODUCTION..... 2

PURPOSE AND SCOPE 2

DESIGN OF THE MCAST WIFI SERVICES..... 2

1. EXTENT OF THE MCAST WIFI SERVICE 3

2. POLICY & APPROPRIATE USE 3

3. CRIMINAL ACTIVITY 4

4. OTHER TERMS 4

5. POLICY NON-COMPLIANCE..... 4

6. DEFINITIONS 5

Introduction

MCAST manages a number of wireless hotspots in designated areas on campus. The service enables College staff, students and visitors to connect to the campus network using laptops, tablets, smartphones and other devices supporting wireless connections.

Purpose and Scope

All users employing wireless methods of accessing MCAST technology resources must adhere to the College’s defined processes for doing so, using MCAST approved access points. Wireless networks are not a replacement for a wired network. Since the College's wireless network is not an extension to the existing wired network, wireless access should not be used for work sessions that require the transfer of large amounts of data (e.g., backups or file downloads) or for access to sensitive organizational data.

Design of the MCAST WiFi Services

The wireless network managed by MCAST is also designed to enhance seamless roaming between access points within and between many buildings and outdoor areas.

The MCAST wireless network is not designed to support latency intolerant applications such as VoIP over Wi-Fi. The MCAST wireless network is designed as an "open" network, which means there is no network-level data encryption or authentication requirement to access the network. The wireless network should be used primarily for general functions such as Web browsing and email. It is not designed to efficiently support high-bandwidth applications such as, but not limited to, streaming media or large file transfers. Wireless "access points," which are located throughout many buildings and common areas, allow compatible wireless devices to connect to the Internet.

Wireless bandwidth is shared by everyone connected to the MCAST WiFi network. As the number of wireless connections increase, the bandwidth available to each connection decreases and performance deteriorates. Distance from the access point, buildings or objects shielding the access point, signal interference, quality of your equipment, battery power and other factors may also impact performance. Applications that generate high network traffic do not work well on wireless networks and negatively impact performance for everyone connected to the same access point.

| | | | | | |
|-----------------|---------------------|-------------------|---|-------------|--------|
| Document Title | Wi-Fi POLICY | | | Page 3 of 5 | |
| Document Number | 182 | Document Revision | A | Date Issued | 8/8/14 |

1. Extent of the MCAST WiFi Service

1.1 Use of Internet services over Wi-Fi is carried out entirely at your own risk.

1.2 MCAST has no responsibility for, or control over, the Internet Services you access and do not guarantee that any services are error or virus free.

1.3 MCAST has no responsibility for, or control over, the information you transmit or receive via the service.

1.4 MCAST does not guarantee:

1.4.1 the availability of the Service;

1.4.2 the speed at which information may be transmitted or received via the Service; or

1.4.3 that the Service will be compatible with your equipment or any software which you use.

1.5 Whilst we take reasonable steps to ensure the security of the Service and to prevent unlawful access to information transmitted or received using the MCAST WiFi Service we do not guarantee the security of the information which you may transmit or receive using the Service or located on any equipment utilizing the Service and you accept that is your responsibility to protect your information and have adequate security (in terms of equipment and procedures) to ensure the security, integrity and confidentiality of your information and data.

1.6 We reserve the right at all times to withdraw the Service, change the specifications or manner of use of the WiFi Service, to change access codes, usernames, passwords or other security information necessary to access the service.

2. Policy & Appropriate Use

2.1 You must not use the Service to access Internet Services, or send or receive e-mails, which:

2.1.1 Are defamatory, threatening, intimidatory or which could be classed as harassment;

2.1.2 Contain obscene, profane or abusive language or material;

2.1.3 Contain pornographic material (that is text, pictures, films, video clips of a sexually explicit or arousing nature);

2.1.4 Contain offensive or derogatory images regarding sex, race, religion, colour, origin, age, physical or mental disability, medical condition or sexual orientation;

2.1.5 Contain material which infringe third party's rights (including intellectual property rights)

2.1.6 In our reasonable opinion may adversely affect the manner in which we carry out our business; or are otherwise unlawful or inappropriate;

2.2 Music, video, pictures, text and other content on the internet are copyright works and you should not download, alter, e-mail or otherwise use such content unless certain that the owner of such works has authorised its use by you.

2.3 We may terminate or temporarily suspend the Service if we reasonably believe that you are in breach of any provisions of this agreement including but not limited to clauses 2.1 to 2.2 above.

| | | | | | |
|-----------------|---------------------|-------------------|---|-------------|--------|
| Document Title | Wi-Fi POLICY | | | Page 4 of 5 | |
| Document Number | 182 | Document Revision | A | Date Issued | 8/8/14 |

- 2.4 We recommend that you do not use the service to transmit or receive any confidential information or data and should you choose to do so at your own risk.
- 2.5 The Service is mainly intended for research purposes. In the event that you use the Service for commercial purposes we would specifically refer you to clause 4.1 below.
- 2.6 All wireless access points within the MCAST must be approved and centrally managed by the IT Department. The addition of new wireless access points within campus facilities will be managed at the sole discretion of MCAST. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment on campus premises, are strictly forbidden.
- 2.7 The IT department will occasionally conduct sweeps of the wireless network to ensure there are no rogue access points present.
- 2.8 The IT department reserves the right to turn off and/or disconnect without notice any access point/equipment connected to the network that it feels puts the college's systems, data, and users at risk.
- 2.9 Any device or equipment found to be interfering with access point signals may be subject to relocation or removal.
- 2.10 Wireless access users agree to immediately report to the IT Department any incident or suspected incidents of unauthorized access point installation.

3. Criminal Activity

- 3.1 You must not use the Service to engage in any activity which constitutes or is capable of constituting a criminal offence, either in Malta or in any state throughout the world.
- 3.2 You agree and acknowledge that we may be required to provide assistance and information to law enforcement, governmental agencies and other authorities.
- 3.3 You agree and acknowledge that we keep a log of the internet Protocol ("IP") addresses of any devices which access the Service, the times when they have accessed the Service and the activity associated with that IP address.
- 3.4 You further agree we are entitled to co-operate with law enforcement authorities and rights-holders in the investigation of any suspected or alleged illegal activity by you which may include, but is not limited to, disclosure of such information as we have (whether pursuant to clause 3.3 or otherwise), and are entitled to provide by law, to law enforcement authorities or rights-holders.

4. Other Terms

4.1 Whilst we do not seek to limit our responsibility for fraudulent misrepresentation, we have no responsibility (to the extent permitted by law) for any direct loss arising from disclosure of confidential information, loss arising from or in connection with use of the service or inability to use or access the service or a failure, suspension or withdrawal of all or part of the service at any time or for any other similar direct loss that may arise in relation to this policy whether or not we were advised in advance of the possibility of such loss or damage.

5. Policy Non-Compliance

Failure to comply with the MCAST Wireless Access Policy may result in the suspension of wireless access privileges and possible disciplinary action.

| | | | | |
|-----------------|---------------------|-------------------|---|-----------------------|
| Document Title | Wi-Fi POLICY | | | Page 5 of 5 |
| Document Number | 182 | Document Revision | A | Date Issued 8/8/14 |

6. Definitions

6.1 Wi-Fi: Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections.

6.2 VoIP: *VoIP* is a technology that allows telephone calls to be made over computer networks like the Internet.

6.3 Access Point: a wireless access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards

6.4 Rogue Access Points; A rogue access point (rogue AP) is any wireless device that has been installed on a network's wired infrastructure without the consent of the network's administrator or owner, thereby providing authorized wireless access to the network's wired infrastructure.

I confirm that I Accept these terms and conditions as the basis of my use of the wireless internet access provided.

Signed:

Name:

E-mail:

Dated: