St Joseph's Theological Institute NPC
(Company number **2003/009125/08**. PBO number **930007111**)
Registered with the Department of Higher Education and Training as a Private Higher Education Institution under the Higher Education Act, 1997 (Registration Certificate number 2003/HE08/003).

Private Bag 6004,
Hilton, 3245
Republic of South Africa
website: www.sjti.ac.za
Telephone: +27(87) 353 8940
Facsimile: +27(86) 435 2264
email: president@sjti.ac.za

WIRELESS POLICY

Title	Wireless Policy
Policy No.	SJTI/ICT/007
Compiled by	ICT Consultant
Provisionally Approved by	President, January 2016
Reviewed and approved by	Board of Directors
Review date	12 October 2017
Responsibility for update	ICT Consultant
Next Review	October 2020

1 INTRODUCTION

1.1 Wireless networking is a fast emerging technology and is set to continue to grow for the foreseeable future. It is recognised that wireless networking could offer benefits to the Institute community in the pursuit of its primary objectives. The recent ratification of further 802.11 standards for wireless access will continue to develop interest in the technology which is by its nature relatively straight forward to deploy. While this may be true and suitable for some environments, wireless LANs within the Institute form part of the bigger infrastructure which includes the wired network. In order to protect the business needs of the Institute the wireless network must meet the same level of security employed by the rest of the infrastructure.

This policy is to ensure that the deployment of wireless networking is controlled and managed in a centralised way to provide functionality and optimum levels of service whilst maintaining network security. It can no longer be acceptable practice to allow the installation and operation of wireless devices on campus without a clear and agreed policy outlining the roles and responsibilities of all parties.

This policy sets out a framework to deal with these issues. The intention of this policy is to define roles and responsibilities for the design of any emerging wireless network, the installation, registration and management of wireless access points, adequate management and allocation of the wireless frequency spectrum and the services offered to end users for wireless access.

1.2 The Policy is maintained and regulated by the Institute's ICT Consultant.

1.3 The Policy is cross-referenced to other Institute policies and the Institute ICT Regulations. Copies of these policy statements are obtainable from the ICT Consultant's office.

1.4 The Policy will be reviewed and if necessary amended from time-to-time, with particular regard to the expected developments in wireless technology and operational use within the Institute, and by reference to the development of recognised best practice.

2 RATIONALE PURPOSE

2.1 This Policy outlines a common set of procedures and operational criteria, in order to effectively manage 802.11 wireless LANs. Due to the characteristics of wireless technology, all wireless developments must be planned, deployed and managed in a careful and controlled manner, and developed in accordance with the Institute's computer and standardisation initiative (see Appendix A). The ICT Consultant has to address the topic of wireless deployment in order to avoid certain issues. There are three main issues this policy aims to address:

Interference. 802.11 wireless technology uses frequencies from a band which is divided into channels. In order for adjacent access points to work with each other and not cause interference, a different channel must be used for each Access Point (AP). Although there are multiple channels within the band, only three are non-overlapping and can guarantee a signal free from interference. It is therefore required that the appropriate channel is assigned to the AP by the ICT Consultant in order to avoid any interference related performance issues.

Security Problems. Wireless LANs offer connectivity to anyone within range of an Access Point; physical boundaries are no longer a relevant option for preventing access to the network. Installation of non-approved devices with little or no security which, if connected to the Institute network, would breach the security of the main infrastructure allowing any unauthorised user with appropriate equipment to connect.

Danger of Device Diversity. Non-standard or misconfigured wireless devices can cause disruptions to the wireless LANs and subsequently the wired network. St Joseph's Theological Institute therefore prohibits the installation of any non-standard wireless access points. This policy is to centralise the purchase and installation of wireless equipment to ensure that inappropriate devices are not installed and used on the Institute's network.

2.2 The Policy describes the standards that users are expected to observe when using Institute wireless facilities, and ensures that users are aware of the consequences attached to inappropriate use of the facilities.

2.3 The Policy also specifies the actions that the Institute will take in the investigation of complaints received from both internal and external sources, about any unacceptable use of Institute wireless facilities.

3 POLICY STATEMENT

3.1 ***Scope of the Policy***

This wireless policy applies to all areas of wireless connectivity to the Institute network infrastructure, and includes all wireless devices operating within the Institute IP address range, on any of the Institute premises, or any remote location directly connected to the campus network.

The ICT Consultant is currently responsible for the Institute's network infrastructure. The wireless network is an extension to this network and therefore the ICT Consultant has the sole responsibility for the design, deployment and management of the Institute wireless LANs.

3.2 ***Policy Restrictions***

i. All Access Points must abide by all national regulations relating to Wireless Devices.

ii. All existing Access Points must conform to recommended specifications as defined by the ICT services.

iii. All new Access Points must be purchased via ICT services, in line with St Joseph's Theological Institute's current purchasing policy and Institute's ICT Standardisation initiative.

iv. All Access Points must follow the ICT Services Standard Configuration settings for Access Points.

v. Access Points will only support the 802.11b and 802.11g standards.

vi. ICT Services prohibit the installation of any non-standard Access Points.

vii. In line with the ICT Regulations (see Appendix B below) ICT services has the right to disable any non-standard device which may cause interference with existing approved Access Points. The offending device may be removed without prior notice.

viii. Proactive monitoring of wireless networks is undertaken by ICT Services on a regular basis and any unauthorised Access Point will be removed from the network.

ix. Any future request for installation of new Access Points must be directed through the ICT consultant.

x. ICT services acts as the central management body in regulating the installation and maintenance of all 802.11 wireless LANs.

3.3 ***Appropriate and Proper Use***

St Joseph's Theological Institute supports the appropriate and proper use of services and facilities that the Institute provides for its students, staff and other authorised users.

3.4 ***Regulatory Framework***

Associated with the provision of these services and facilities, St Joseph's Theological Institute takes seriously its responsibility to provide an appropriate regulatory framework, including specific standards and guidance for the appropriate use of these Institute services and facilities. The Wireless Policy constitutes a component part of this regulatory framework.

Use of all ICT facilities provided by St Joseph's Theological Institute is subject to the relevant Policies and Regulations, in particular the Institute ICT Regulations and the Institute Internet Policy Statement.

3.5 ***Acceptance of Policies and Regulations***

It is a condition of use of ICT facilities provided by St Joseph's Theological Institute, by a student, member of staff or any other authorised person, that the user agrees to be bound by the relevant Institute Policies and Regulations.

4 ROLES AND RESPONSIBILITIES

4.1 All Wireless LANs are monitored and maintained by the ICT Consultant. Any Access Point which is connected to the Institute network infrastructure becomes the responsibility of the ICT Consultant.

4.2 User Responsibilities
The following specific responsibilities apply to users of the Institute's wireless network:

i. Users of the wireless network are responsible for their own computer equipment. The Institute accepts no responsibility for any loss or damage to personally owned machines as a result of connection to the wireless network.

ii. Users have the responsibility to ensure that they are running up to date antivirus software and that the operating system is fully patched with the latest service packs and updates.

iii. Users will authenticate on the wireless network for each session.

Appendix A – Institute Computer Standardisation Recommendations

In order to protect the business needs of the Institute and to minimise any risk of damage to the security or integrity of Institute systems, all developments of the Institute network infrastructure must be in compliance with approved standards and approved by the ICT services/consultant.

For the avoidance of any adverse interaction with the Institute network, the provision and operation of any wireless networks in the Institute separate from the main network must also be in compliance with approved standards and agreed in advance of purchase with ICT Services.

Appendix B – ICT Regulations

Users must not connect any unauthorised equipment to the Institute network without consultation and the prior written approval from the ICT services. If the ICT services has reasonable grounds for believing that any equipment may be the cause of unacceptable degradation of the performance of the network detrimental to other Users, then the User must co-operate with the disconnection of the equipment from the network pending resolution of the problem.

Appendix C – Glossary of Terms

802.11
Refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and an access point or between two wireless clients.

802.11a
Operates in the 5 GHz frequency range (5.125 to 5.85 GHz) with a maximum 54Mbit rate. The 5 GHz frequency band isn't as crowded as the 2.4GHz frequency because it offers significantly

more radio channels than the 802.11b and is used by fewer applications. It has a shorter range than 802.11g, is actually newer than 802.11b and isn't compatible with 802.11b.

802.11b
Operates in the 2.41 GHz Industrial, Scientific and Measurement (ISM) band (2.4 to 2.4835 GHz) and provides rates of up to 11Mbit/sec. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz ISM band.

802.11g
Similar to 802.11b, but this standard supports data rates of up to 54Mbit/sec. It also operates in the heavily used 2.4 GHz ISM band but uses a different radio technology to boost overall throughput. It is compatible with 802.11b.

802.1X
As the IEEE standard for access control for wireless and wired LANs, 802.1x provides a means of authenticating and authorising devices to attach to a LAN port. This standard defines the Extensible Authentication Protocol (EAP), which uses a central authentication service to authenticate each user on the network.

Access Point (AP)
is a WLAN transceiver or "base station" that can connect a network to one or many wireless devices. APs can also bridge to one another. Wireless devices, such as laptops or PDAs, connect to a wired LAN via an AP, which is a hardware device or a computer's software that acts as a communication hub. APs provide heightened wireless security and extend the physical range of a wireless LAN

Extensible Authentication Protocol (EAP)
is an 802.11x standard that allows developers to pass security authentication data between RADIUS and the AP and wireless client. EAP has a number of variants, including EAP MD5, EAP-Tunnelled TLS (EAP-TTLS), Lightweight EAP (LEAP), and Protected EAP (PEAP)

Site Survey
is undertaken at the location for a new wireless LAN in an effort to avoid what could be time-consuming and costly problems during deployment. It involves diagramming the network, checking the building and testing the equipment.

WEP (Wired-Equivalent Privacy)
protocol was specified in the IEEE 802.11 standard to provide WLAN with a minimal level of security and privacy comparable to a typical wired LAN, using data encryption. It's now widely recognised as flawed because of an insufficient key length and other associated problems.

Wi-Fi (Wireless fidelity)
the generic term for 802.11 technology Wireless LAN used radio frequency technology to transmit network messages through the air for relatively short distances, like across an office building or college campus. A wireless LAN can serve as a replacement for or more usually an extension to a wired LAN.

WPA (Wi-Fi Protected Access)
is a data encryption specification for 802.11 wireless networks that replaces the weaker WEP. It improves on WEP by using dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions.


SJTI