UNIVERSITY of the WESTERN CAPE	**UNIVERSITY OF THE WESTERN CAPE**		
	Wireless LAN (WiFi) Policy	Council Approval Reference No.	C 2004/5)
		Implementation Date	May, 2004
		Revision / Amendment Number	1
		Revision / Amendment Date	
		Policy Owner	Director: ICS
		Executive Management Portfolio	Exec. Director: F.I.O.I
		Contributors	ICS Senior Leadership Team;
		Circulated by:	Head: IT Strategy & Planning
		Circulated to:	ICT PSC; ICT GC

	UNIVERSITY OF THE WESTERN CAPE		
UNIVERSITY of the WESTERN CAPE	**Wireless LAN (WiFi) Policy**	Council Approval Reference No.	C 2004/5)
		Implementation Date	May, 2004
		Revision / Amendment Number	1
		Revision / Amendment Date	
		Policy Owner	Director: ICS
		Executive Management Portfolio	Exec. Director: F.I.O.I
		Contributors	ICS Senior Leadership Team;
		Circulated by:	Head: IT Strategy & Planning
		Circulated to:	ICT PSC; ICT GC

1. Executive Summary

It is recognised that wireless connectivity services offer benefits to the University and its affiliates and guests through delivery of flexible access and communication services.

The Wireless LAN (WiFi) policy provides the framework for the implementation of wireless connectivity services at the University of the Western Cape (UWC), which includes determination of identity and authentication to ensure the provision of appropriate levels of security when accessing the UWC WiFi facilities.

Due to a wide range of mobile devices, legacy technologies and manufacturers in the market place, the policy aims to address the conditions and limitation of support on the UWC Wireless LAN commonly termed as WiFi.

2. Definition of Terms within the Policy

Unless the context otherwise indicates:

"Access Point" ("AP") is the device that forms part of a wireless network and to which users using wireless devices connect to gain network access.

"BYOD" "Bring your own Device" is the practice of allowing staff or students of the institution to use their own computers, smartphones, or other devices on the UWC network for work or academic purposes.[1]

"IEEE 802.11x" is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.[2]

"**Rogue access point**" is a wireless access point that has been installed on a secure network without explicit authorisation from a local network administrator.

"Authorised Users" are all users who have been granted rights to utilise the University's wired and wireless connectivity services based on a legitimate need within the context of the University's Academic mission. This may include University staff, students, contractors and third-party agents.

"**Wireless LAN (WLAN)**" is the network that allows wireless enabled devices to connect and communicate via WiFi.[3]

UNIVERSITY OF THE WESTERN CAPE			
UNIVERSITY of the WESTERN CAPE	**Wireless LAN (WiFi) Policy**	Council Approval Reference No.	C 2004/5)
		Implementation Date	May, 2004
		Revision / Amendment Number	1
		Revision / Amendment Date	
		Policy Owner	Director: ICS
		Executive Management Portfolio	Exec. Director: F.I.O.I
		Contributors	ICS Senior Leadership Team;
		Circulated by:	Head: IT Strategy & Planning
		Circulated to:	ICT PSC; ICT GC

"**WiFi"** is a trademark reference to the suite of IEEE 802.11x network technology protocols that allow transmission between devices using radio waves.

3. Scope

1. This policy applies to all Authorised Users who access the University's wireless LAN (WiFi) connectivity services.
2. The policy applies to WiFi services offered on all the University's campuses and in buildings / facilities under its management.

4. Purpose

1. The Wireless LAN (WiFi) Policy aims to set out the conditions for the provisioning of the UWC WiFi connectivity service and to inform users of their role and responsibilities in relation to their use of the WiFi service.

5. Policy statement

1. The University of the Western Cape (UWC) deploys Wireless LAN (WiFi) connectivity services in the University's buildings and certain outdoor areas on its campuses, and in offsite buildings under the University's management, in support of its Academic mission, which includes Learning and Teaching, Research, Community Engagement and various Professional, Administrative and Operational support services,
2. UWC's WiFi connectivity service is provided to staff and students for the primary purpose of conducting work, research and community engagement as related to the Academic Programme and Administrative support functions of the University.
3. The use of UWC WiFi for purposes that are not in the University's interests, is prohibited, e.g. to conduct private business.
4. The UWC WiFi policy requires that all WiFi infrastructure be authorised by the Information and Communication Services (ICS) department, e.g. installations, maintenance, additions, enhancements, replacements, adjustments and removals.

6. Security Warning

1. The University does not guarantee the privacy of data and communication while using the WiFi service as there are potentially serious threats to any computer device connected to the internet without the appropriate security protection. These threats range from malware that can damage the device to attacks on the device by unauthorised third parties.
2. By using the WiFi service, users acknowledge and knowingly accept these risks, and agree to using the WiFi service at their own risk.

7. Disclaimer

By using the UWC WiFi service, users agree to the terms set forth in the following disclaimer:

1. **Service provided As-is -** This Service provided to the Internet is on an as-is basis with all the risks inherent in such access. UWC makes no warranty that the WiFi service, or that any information, software, or other material accessible on the WiFi service, is free of viruses, worms, Trojan horses or other harmful components. By connecting, the user acknowledges and accepts the risks associated with access to the Internet and use of a wireless network.
2. **Service provided As-available -** The Service is provided on an as-available basis without warranties of any kind, either expressed or implied, that the Service will be uninterrupted or error-free including, but not limited to, vagaries of weather, disruption of service, acts of God, warranties of title, nor implied warranties of fitness for a purpose. No advice or information given by the University, its affiliates, contractors or their respective employees shall create such a warranty.
3. **Indemnity –** Users of the WiFi service agree to indemnify and hold harmless UWC, and its affiliates, agents, and contractors, from any claim, liability, loss, damage, cost, or expense that result in any way from users' use of, or inability to use, the WiFi service, or to access the Internet or any part thereof, or users' reliance on or use of information, or services provided on or through the WiFi service and/or any materials downloaded or uploaded through the WiFi service, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation, or any failure of performance, or any violation of any third party's rights or a violation of law or regulation.

8. Policy provisions

A. General

1. The Information and Communication Services (ICS) department of UWC has been mandated by the University's Executive with overall responsibility for the proper deployment and management of the WiFi connectivity service, including infrastructure elements and radio frequency (RF) spectrum use.
2. The UWC WiFi service is considered a complementary network connectivity service to the primary wired Local Area Network (LAN) connections.
3. UWC offers a standard wireless deployment plan that meets the needs of most departments wishing to utilise WiFi access services.
4. WiFi infrastructure deployed by the University is designed to operate harmoniously with existing networks. The WiFi network is also designed to provide seamless roaming between wireless access points within and between buildings, and outdoor areas.
5. The ICS department endeavours to deploy WiFi services across all areas and/or buildings of the University, subject to the outcome of feasibility studies and the commitment of the necessary resources.
6. UWC WiFi services will adhere to appropriate security standards for access control, which will be reviewed and refined to ensure alignment with evolving industry standards.
7. Installation of departmental or DIY WiFi infrastructure and services are prohibited to avoid interference with the UWC WiFi network, unnecessary impact to the wired network and to minimise undue security risks to the University.
8. No department or individual may deploy WiFi infrastructure making use of the 802.11 standards without obtaining written approval from the University's appropriate Governance structures.
9. The University reserves the right to optimise performance and minimize interference to the UWC WiFi network and may disable and remove rogue wireless infrastructure and/or disable WiFi network access in certain areas for a variety of reasons, including abuse of the WiFi service through excessive bandwidth usage, a misconfigured or compromised device or degradation of service to other users.
10. UWC reserves the right to respond, without notice, to Information Security threats that are deemed to place the University's systems, data, and/or users at risk. Such responses may include disabling wireless infrastructure connected to the University's network.

B. Supported Technology

1. The WiFi network services are based on the IEEE 802.11 international standards.
2. UWC does not guarantee wireless connectivity for all mobile devices due to the eclectic mix of mobile devices as a result of the "Bring Your Own Device" (BYOD) policy on campus.
3. Backward compatibility of older-generation mobile devices, not compatible with the wireless standard currently deployed, falls outside the scope of UWC's support.

C. Quality of Service and Usage

1. Use of the UWC WiFi network is subject to the University's ICT Computer, Internet and Email Usage Policy.
2. The UWC WiFi service is a shared medium with throughput efficiency closely linked to the number of users and downloads/uploads via an access point.
3. The user experience may therefore be influenced by the number of users connected to an access point and the volume of downloads and/or uploads that may flow through these access points, at a given point in time.
4. The University reserves the right to implement bandwidth restrictions to prevent abuse of the UWC WiFi service and/or to manage a consistent quality of service to users.
5. The University is not obliged to provide personal, third-party application support. There are numerous mobile applications, hardware manufacturers and operating systems available and the University cannot guarantee their full functionality and use on the UWC WiFi network.

9. Policy Non-compliance

1. All users of the University's WiFi network service, including staff, students, contractors, external third parties and/or agents, must comply with the policy and supplementary policy documents and guidelines, and must keep abreast of updates to these policies.
2. Violation and/or failure to comply with the policy may result in network access revocation, corrective action, and/or civil or criminal prosecution, depending on the nature of the violation.
3. Violators may be subject to disciplinary action pursuant to University policies, collective bargaining agreements, codes of conduct, or other instruments governing the individual's relationship with the University. Violation of this policy and supplemental policies, standards and procedures may also be reported to external parties as required by law.

4. Third party vendors and service providers found to have violated this policy may incur financial liabilities, in addition to termination of contract.
5. Recourse shall be available under the appropriate section of the University's disciplinary procedures, the employee's personnel contract, or by pursuing applicable legal procedure.

10. Relevant Statutes

1. The University has an obligation to comply with relevant legal and statutory requirements, and this policy, and supplementary policy documentation, aims to promote compliance with applicable laws by providing directions and guidelines to underpin the University's compliance with these laws. Applicable laws and legislation include, but are not limited to:
   1.1. The South African Electronic Communications and Transactions Act (Act No. 25 of 2002) – this protects personal information that has been obtained via an electronic medium.
   1.2. Protection of Personal Information Act (POPIA) (Act No. 4 of 2013).

11. Related Policies and Procedures

I. Related Policies

A. Bandwidth Management Policy (C 2011/2);
B. ICT Computer, Internet and Email Usage Policy (C 2017/3);
C. ICT Information Security Policy (C 2017/3)
D. Password Policy (ICS) – (C 2005/3)

12. Relaxation and Exceptions

All requests for relaxations and/or exceptions to this policy must be submitted to the ICS service desk via email to **servicedesk@uwc.ac.za.**

13. Revision Cycle

The Office of the Director: ICS will be responsible for this policy. This policy will be reviewed by ICS, and changes will be authorised by endorsement of the ICT Governance Committee and approval by UWC Council.

14. Annexures / Appendices

1. Unacceptable Use of the WiFi network

In order to protect UWC from any liability due to the misuse and abuse of our electronic communications facilities including WIFI, ***users may not:***

- View, store or distribute any material that is sexually explicit, pornographic, racist, sexist, or derogatory of race, origin, sex, sexual orientation, age, disability, religion or political beliefs.
- View, store or send messages intended to harass, intimidate, threaten, embarrass, humiliate or degrade staff or students or that contain defamatory references.
- Download, install, store or distribute pirated software or videos, entertainment software, music or games.
- Intentionally propagate viruses, worms, Trojan horse or trap door program codes on the UWC network. (Users have an obligation to ensure their personal devices (BYOD) are periodically updated with the latest anti-malware and anti-virus software.)
- Copy, destroy, delete, distort, remove, conceal, modify or encrypt messages or files or other data on any University computer, network or other communication system without the permission of an authorised individual.
- Attempt to access another staff member, student or contractor's computer, computer account, e-mail or voice mail messages, files or other data without their consent or the consent of an authorised individual.
- Violate or attempt to violate any other applicable laws, prescriptions or provisions.
- Make excessive use of bandwidth-intensive streaming services that disadvantage other authorised users from fair and reasonable access to and use of the UWC WiFi network service.
- Use the UWC WiFi network in a manner that impedes any UWC operational activity.

2. Bandwidth Shaping

In a University environment, Educational, Research and Community Engagement activities must enjoy preferential access to the Internet. Certain areas / users, however, generate considerable usage that falls outside these focal areas, (e.g. peer-to-peer file sharing, streaming services, multi-media downloads etc.) that may potentially impede the performance and user experience of access required for the University's core functions.

Thus, the objective of bandwidth shaping on UWC Internet access is to ensure that the University's core business traffic, and other prioritised traffic types receive preferential treatment in the event of network congestion.

It also enables us to dynamically allocate bandwidth for important activities / events on campus.

Restrictions have been imposed on low priority traffic types while other non-compliant sites / content – e.g. pornography, are blocked.

3. Special cases

Notwithstanding the enforcement of the Wireless Policy, ICS recognizes that there are special cases where some of the bandwidth management principles may not apply, or may need to be applied differently from the rest of campus. This includes postgraduate and research areas that make extensive use of the Internet, for example in computer science, information systems, bio-informatics, GIS, landscape ecology, and others.

ICS will endeavour to meet the special requirements of such areas in the best possible manner while maintaining the integrity of the campus' operational network. Any allowances made for special cases will be subject to the availability of funds to meet additional costs that may be incurred.