Policy on Use of the Wireless Infrastructure

Title:	Use of the Wireless Infrastructure
Policy number:	POL 014
Approval(s) required	Academic Senate ☐ Board of Trustees ☒ Both ☐
Date of Senate approval if required	(dd/mm/yyyy)
Date of Board approval if required	06/12/2023
Effective date of implementation	06/12/2023
Frequency of review required	2 years
Replacing or superseding information	Policy name(s) and number(s) that this policy replaces. When a new policy supersedes part of an earlier policy, the partially superseded policy should be revised and approved so as to avoid potentially conflicting policies.
Revision number	New
Responsible Office	Office of Information Technology
Accountable Officer	Vice President, Information Technology/Chief Information Officer
Related legislation, regulation, policy, or policies	Policy on Acceptable Use
Appendix/Appendices	None.

1. Authority

Board of Trustees.

2. Purpose

To educate on how the wireless infrastructure is to be used.

3. Scope

This policy applies to all employees (permanent, contractual, and temporary), students, guests of the University, and any other third parties using equipment provided by the University of The Bahamas.

4. Definitions

Wi-Fi: a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet. It allows these devices--and many more--to exchange information with one another, creating a network.
Internet connectivity occurs through a wireless router. When you access Wi-Fi, you are connecting to a wireless router that allows your Wi-Fi-compatible devices to interface with the Internet.

Wireless local-area network (WLAN): a group of co-located computers or other devices that form a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN; anyone connected to Wi-Fi while reading this webpage is using a WLAN.

Access Point: electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a LAN using transmits, and receives antennas instead of ports for access by multiple users of the wireless network

Wireless Infrastructure: wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

Coverage: the geographical area where a baseline level of wireless connection service quality is attainable.

Interference: the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.

Privacy: the condition that provides for the confidentiality of personal, student, faculty, and staff communications, and institutional data transmitted over a wireless network.

Client hardware/software: the electronic equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device to provide a LAN interface

5. Policy Statement

5.1. Overview

5.1.1. Wireless equipment and users must follow all network connection policies as set forth in the policy herein. All provisions of the IT Security Requirements and Practices apply to this policy.

5.1.2. Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited

5.1.3. Wireless access points must abide by all laws, rules, and/or regulations pertaining to wireless networks.

5.1.4. Deployment and management of wireless access points in areas not controlled by the university's IT department are not the responsibility of the IT department or the university.

5.1.5. Wireless access points shall require user authentication at the access point before granting access to campus or Internet services. Wireless network interfaces and end-user devices shall support authentication to access wireless networks that allow connectivity to the Campus Network.

5.2. **Network Access Points**

5.2.1. All installed wireless access points and antennas are the property of the University. Do not tamper with, adjust, abuse, repair, or otherwise touch these access points and their antennas.

5.2.2. All dormitory residents must be aware that the dormitories are equipped with wireless access points and antennas. Due to the presence of this equipment, residents should be very careful not to damage this equipment through their activities in these areas. Students may not attempt to probe, scan, or test the vulnerability of any system or network, or breach security or authentication measures, which include attempting to obtain and/or distribute encryption keys used at the University.

5.2.3. Students are not allowed to set up any form of proxy service or other such arrangement to enable more than one computer to access the network via a wireless connection; each student is limited to one connection. In addition, students are not allowed to set up any type of server or server operating system on computers that are connected to the network. This includes, but is not limited to, the following services:

- DHCP – Dynamic Host Configuration Protocol
- WINS – Windows Intenet Name Service
- DNS – Domain Name System
- Web Servers

5.2.4. Students must remember that the network is a shared resource and that many people must use it for their daily work. Consuming large amounts of system resources (network bandwidth, disk space, print queues) by performing large file downloads or networked gaming can obstruct this work, and in such cases the University's IT staff has the authority to throttle bandwidth and/or terminate connections that monopolize resources.

5.3. **Dorm Connectivity**

5.3.1. Students have access to the Internet and web access to their email in their dorm rooms provided they possess their own desktop or laptop systems. This privilege is provided by the University and is subject to revocation if the student violates any portion of this policy and agreement, or if dorm Resident Assistants, faculty, staff, and and/or instructors assess that the privilege interferes with the primary educational goals of the student, or is not consistent with the mission of the University.

5.3.2. Technical support services provided by the IT Department are limited to campus Internet connectivity. The University's computer technicians are not responsible for privately owned hardware or software problems that affect a computer's/laptop's/notebook's ability to connect to our network. The IT Department will not be responsible for repairing hardware/software problems on a student's personal computer. In addition to the stated regulations and guidelines of this Policy, students who use this option of connectivity must abide by the following rules:

- Any bandwidth sharing device or wireless signal repeater (i.e., Airport Express, routers, switches, hubs or wireless means) is not allowed.
- Telephone/Modem Internet access is not allowed.
- Illegally sharing music or video files over the network is prohibited.

5.4. **Acceptable Use**

5.4.1. The major purpose of supplying Internet, wireless connectivity, and electronic mail, whether in academic facilities or in the dorm, is to enhance learning and communication for the members of the University community. Research on the Internet, the receipt and submission of assignments via e-mail, or sending e-mail to teachers, experts in various fields of study, family, and friends are allowed. The University also permits use of these services for pursuing topics of personal interest or for entertainment, provided the activities fall within the guidelines specified in this document.

5.5. **Unacceptable Use**

5.5.1. Users may not use the University's network to access computer files not belonging to them, copy or transfer computer software where this constitutes software piracy, violate copyright law, use the network for commercial activity or financial gain, or use the network for any illegal purpose. See Acceptable Use Policy.

5.6. **Policy Violations**

5.6.1. Violators of the above-stated policy will be subject to one or more of the following disciplinary actions:

- Violators may receive a written notice and warning about the violation.
- The violator's network connection may be immediately terminated.
- Network access may be suspended until the situation is rectified.
- Network access may be suspended for a specified period of time.
- Replacement/repair costs for damage to University owned property will be charged to the responsible violator's account.
- Violations by students may be reported to the Dean of Students, which may result in further, more serious, penalties.
- Failure to comply with any of the above policies may result in termination of Campus WiFi services, loss of computer use privileges, prosecution by the University based on the University's standards of disciplinary violations for students, standards of disciplinary procedures for faculty and staff, and/or judicial prosecution.

- The University reserves the right to terminate any wireless connection without notice should it be determined that said connection infringes on University security or inhibits or interferes with the use of the University's network by others.

5.7. **Disconnect Authorisation**

5.7.1. Any Wireless Access Point or SSID on campus, which poses a security threat may be disabled from the campus network. Every reasonable attempt will be made to reach the registered "Point of Contact" to resolve security problems. The University's Network Administrator has the authority to disconnect any wireless network from the campus network backbone whose traffic violates practices set forth in this policy, or any network-related policy.

5.7.2. Any user whose connection to the wireless network poses a security threat may be disconnected from the campus network. Every reasonable attempt will be made to notify the user of the reason for disconnection. The owner of the device is expected to have their device repaired. Once completed, the user may contact the Office of Information Technology (OIT) through the IT Help Desk to request reconnection.

5.7.3. Grievance matters with this policy or conflicts should be directed to the Office of Information Technology through the IT Help Desk for attention. The Office of Information Technology should be notified within one week of the incident in question. If the conflict is not resolved to the satisfaction of grievance initiator, the department, or division, the matter may be escalated to the Information Technology Committee for further review and action.

6. History

The history table documents significant changes so that the evolution of the policy is recorded.

Revision	Date	Changes to Policy/Comments
new		