LIFE CHIROPRACTIC
COLLEGE WEST

# Campus Policy on the Use of WiFi

Planning, Technology & Special Projects

February 2019

## I. Purpose

The wireless network on campus is a resource for educational technology and instruction. This policy provides requirements for access to and use of this shared resource in order to provide the best possible educational and learning experience for students, faculty and staff. This policy also establishes protections and requirements intended to secure the entire network of the college from intrusion of malicious software, data loss, and degradation of the system performance.

## II. Use of the campus WiFi

Use of the campus wireless network is prioritized to support educational and operational needs, maintain the highest possible security against risks, and provide a satisfactory, convenient personal experience for visitors, students, and staff when outside of the educational and instructional sessions. Rogue devices severely degrade system performance and can possibly introduce malicious software. The prevention of such incidents is achieved by imposing limitations on the use of the campus wireless network.

A. No user will create a hot spot on any campus network with any device.
B. No user will introduce equipment or software onto any port or via any wireless access point which assigns IP addresses for other devices. These rogue devices are not recognized by the network as sources to provide addresses to devices for active sessions. They interfere with those network servers which do dynamically assign IP addresses.
C. Updates to device operating systems will be blocked by network policies. Such updates require large quantities of data to be transferred via their connected sessions. Such throughput adversely impacts the active sessions of all other users on the network. Users are required to update their devices at locations and on networks other than those located and maintained on campus.
D. Each of the wireless networks (SSIDs) have restrictions to selected websites to which any active session can connect, transmit and receive data. Use of the SSIDs dedicated to education, learning, and assessment are more restrictive than those available for non-educational or personal use.
E. Accessibility to peer-to-peer (P2P) and data-streaming sites are restricted to those that support collaboration of campus constituents, and the delivery of educational content.
F. Passwords to the wireless networks are to be changed at a frequency appropriate for the security and management of sensitive information required for each network. Passwords for SSIDs are to be changed at least annually.

## III. Networks and their configuration

There are two independent internet service providers (ISPs) for the campus. The primary ISP provides the greater bandwidth, whereas the secondary ISP serves as a redundant internet service in the event the connectivity to the primary provider is interrupted or under maintenance. The total bandwidth is divided into five wireless networks, each with their own characteristics and restrictions.

A. **LCCWStaff** network is password protected and reserved for use by college staff and faculty in support of operational and transactional tasks associated with their jobs. The firewall restrictions placed on LCCWStaff block access to known sites posing security risks, but must allow access to a wide range of websites and configurations of hosted and remotely connected environments.
B. **Lifewest** network is password protected and used by students and visitors for personal internet connectivity.
C. **Guest** network is used by visitors for personal internet connectivity. This SSID requires acceptance of terms of use at the time of login prior to being granted access.
D. **HC_Assessment** network is password protected and dedicated to the collection of data for interns in the campus Health Center during competency examinations and faculty assessments of intern's clinical educational performance. Devices used by observers and raters are restricted to iPads owned, maintained, and managed by the college. No other device is allowed to connect to the HC_Assessment wireless network.
E. **Academic_Assessment** network is password protected and dedicated to the collection of data for students in the academic courses not administered as part of their clinical education experience. The administration of on-line quizzes, surveys, examinations and course evaluations are supported by the Academic_Assessment wireless network. The password is provided to students in order to access the assessment environment housed within the LMS, to authenticate and open the software that blocks internet browsers, and to complete and submit the assessment. Users are allowed to connect with their personal device.

## IV. Copyright protected material

Students and staff are reuired to comply with copyright policy notices posted at copiers and printers. Students and staff who use the college's information technology systems to engage in illegal or unauthorized distribution of copyrighted

materials may be subject to disciplinary action by the college as well as civil and criminal liabilities for violation of federal copyright laws.

## V. Compliance to this policy

The wireless networks are managed and monitored by software installed on the wireless access points (WAPs) and the network switches. These software applications are agent-based controllers licensed and provided by the manufacturers of the equipment. Insight into the behavior and performance of the system is achieved by qualified technicians and network engineers. Unknown and rogue devices are identified, and the software alerts technicians of possible interference or risks of intrusion.

Securing the network is the priority of monitoring the compliance with the provisions of this policy. To ensure compliance while not intruding on the privacy of any one individual, the following guidance and actionable enforcement are established.

A. Disconnection of devices from an active session
B. Deregistration of devices for a user
C. Legal action and compensation of damages incurred from a security breach
D. Administrative action for non-compliance with this policy, resulting possibly in dismissal from enrolled status or termination of employment

## VI. Change Log

Revisions to this policy are documented in this location. A record of the dates of changed passwords and the responsible administrator of the passwords is maintained here. The passwords are not recorded herein.

Rev(0) is the original policy, dated 8 February 2019.

| Section Title | Description of Change | Pages | Rationale for Change/Date |
|---|---|---|---|
| Rev (0) | Original Policy | 1-7 | None / 8 Feb 2019 |
| | | | |
| | | | |

## VII. SSID Configurations

The record of restricted and blocked website and internet sites for each wireless network (SSID) of Life Chiropractic College West is provided here. This table is an integral part of the WiFi policy for users. Updates and revisions to these blocked websites are to be recorded in the Change Log of the preceding section.

| SSID | Allowed Website Name | Blocked Website Name | Effective Date |
|---|---|---|---|
| LCCWStaff | All others | Restricted sites identified and quarantined by Sophos, Proofpoint Essential and ESET anti-virus software | 8 Feb 2019 |
| | | | |
| Lifewest | All others | Restricted sites identified and quarantined by Sophos, Proofpoint Essential and ESET anti-virus software | 8 Feb 2019 |
| | | | |
| Guest | All others | Restricted sites identified and quarantined by Sophos, Proofpoint Essential and ESET anti-virus software | *TBD* |
| | | | |
| HC_Assessment | Qualtrics | ESPN, Disney, Netflix, BitCurrent, Yahoo, Facebook | 8 Feb 2019 |
| | | Restricted sites identified and quarantined by Sophos, Proofpoint Essential and ESET anti-virus software | |
| | | | |
| Academic_Assessment | InstructureCanvas, CAMS Enterprise, Respondus Lock-down Browser | All other sites and destinations | 8 Feb 2019 |
| | | | |