NO. 3058   INFORMATION TECHNOLOGY RESOURCES ACCEPTABLE USE POLICY

1.0   GENERAL PROVISIONS:

1.1   Purpose: Oklahoma City Community College ("OCCC") expects all members of the OCCC community to use Information Technology Resources in a responsible manner. The purpose of this policy is to promote the responsible, ethical, legal and secure use of Information Technology Resources for the benefit and protection of OCCC and Users. These resources may be used only in a manner consistent with the Mission, Values, policies and procedures of OCCC and applicable law. Access to OCCC owned, leased, and contracted Information Technology Resources is a privilege accorded by OCCC. OCCC reserves the right to limit or deny use of and access to its Information Technology Resources.

1.2   Scope: This policy applies to all Users of OCCC Information Technology Resources, including but not limited to OCCC students, faculty and adjunct faculty, staff and retirees, as well as library patrons and other guests of OCCC who access or utilize OCCC Information Technology Resources. This policy applies to the use of all Information Technology Resources as defined below. Personal equipment accessing OCCC information technology resources and all equipment and services owned, leased or contracted by OCCC are subject to this policy.

1.3   Definitions:

1.3.1   Access Point – An Access Point is a hardware device or a computer's software that acts as a communication hub for users to access an Information Technology Resource of OCCC.

1.3.2   Information and Instructional Technology Services (IITS) – IITS is the organizational unit of OCCC that serves and is responsible for the information technology and telecommunications needs of students, faculty and staff of OCCC.

1.3.3   Information Technology Resources – Information Technology Resources include, but are not limited to: (a) OCCC owned or leased software and hardware, e.g., PCs, laptops, PDAs, and other handheld electronic devices; (b) OCCC contracted information services; (c) OCCC local area network (LAN); (d) OCCC wide area network (WAN); (e) OCCC wireless network (WI-FI); (f) OCCC employee, student and retiree e-mail systems; (g) OCCC telecommunication and voice-mail systems; (h) OCCC student information systems (SIS); (i) OCCC learning management systems and subsystems (LMS); (j) OCCC content management systems (CMS); (k) OCCC electronic workflow systems; (l) thin client systems, (m) OCCC Portal; (n) data warehouse/reporting systems, (o) the internet; (p) OneNet systems; (q) information systems and services provided by the Oklahoma State Regents for Higher Education (OSRHE); (r) as well as all facilities, information

resources and contracted services supporting instructional activities or required to accomplish information processing, storage, and communication, whether individually controlled or shared, stand-alone or networked.

1.3.4 Local Area Network (LAN) – The Local Area Network is a computer network that connects workstations, personal computers and information technology resources together. A system of LANs connected in this way is defined as a Wide-Area Network (WAN).

1.3.5 User – A User is defined as any individual who uses or logs into or attempts to use or log into an OCCC system or computer, or who connects or attempts to connect to an OCCC network or system, whether from on campus or remotely.

1.3.6 Wireless Network (WLAN or WI-FI) – A Wireless Network is defined as any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and/or microwaves to maintain communications.

1.4 Terms of Use: By accessing or using, or attempting to access or use, OCCC Information Technology Resources, the User acknowledges and agrees to the following:

1.4.1 A User shall use only those Information Technology Resources the User is authorized to use and only for the purposes authorized. Users shall:

1.4.1.1 Use Information Technology Resources for authorized purposes only;

1.4.1.2 Use only those Information Technology Resources the User is specifically authorized to use and use assigned accounts, transactions, data and processes only for the purposes specifically authorized;

1.4.1.3 Use only their own accounts and passwords. Using someone else's account and/or password without authorization and sharing the User's own account and password with anyone other than authorized IITS personnel are violations of this Policy;

1.4.1.4 Access only those files, data or processes the User is authorized to access;

1.4.1.5 Discontinue the use of former authorized access after use privileges have expired or been revoked or suspended;

1.4.1.6 Refrain from looking for or exploiting security flaws to gain access to the system or data, and attempting to circumvent OCCC security mechanisms;

1.4.2 Users shall not intentionally develop or use programs, transactions, data, or processes that harass or disrupt other Users or infiltrate the system or damage or alter the hardware, software or data components of a system. Alterations to any system or network software or data component shall be made only under specific instructions from authorized personnel. Examples of conduct that violates this policy include but are not limited to:

1.4.2.1 Releasing any virus or worm that damages or harms OCCC Information Technology Resources or any other system or network;

1.4.2.2 Preventing others from accessing an authorized service.

1.4.2.3 Disrupting or impairing OCCC Information Technology Resources or any other college operated system.

1.4.3 Users shall comply with applicable federal, state and local laws, OCCC policies and procedures, and the OneNet Acceptable Use Policy (available at http://www.onenet.net/clientservices/category1/sub3/acceptableuse.htm. For example, by way of illustration but not limitation, Users shall:

1.4.3.1 Respect the copyright and intellectual property rights of others;

1.4.3.2 Make only those copies of licensed software or programs that the license allows;

1.4.3.3 Not download, distribute or use pirated software or programs;

1.4.3.4 Comply with intellectual property and copyright law in downloading uploading, and distributing copyrighted materials, such as music and video files;

1.4.3.5 Not use OCCC Information Technology Resources for private consulting or commercial enterprises, outside employment, self-employment, partisan political purposes and/or personal financial gain. Except as provided in the preceding sentence, personal use by students and library patrons, and reasonable, incidental personal use by employees is permitted, unless otherwise in violation of this policy;

1.4.3.6 Not use Information Technology Resources for the purpose of threatening or stalking other individuals, or for harassment in violation of OCCC's anti-harassment and anti-discrimination policies;

1.4.3.7 Not knowingly access, store, transmit or display obscene or harassing images, messages, or cartoons;

1.4.3.8 Not view, access, upload, download, distribute or possess child pornography;

1.4.3.9 Be sensitive to the public nature of shared facilities, avoiding the display or transmission of images, sounds or messages (including material that could be considered pornographic) which creates an unlawful hostile environment for others;

1.4.3.10 Not transmit libelous or defamatory material, material protected by rights of privacy or publicity, or material protected as trade secrets.

1.4.4 OCCC recognizes academic freedom and responsibilities in the use of Information Technology Resources, as described in OCCC Policy No. 4042, Academic Freedom and Responsibilities.

1.4.5 Users shall comply with the Oklahoma State Regents for Higher Education's Acceptable Use Policy governing OneNet http://www.onenet.net/clientservices/category1/sub3/acceptableuse.htm

and the Office of State Finance [Information Security Policies, Procedures Guidelines at http://www.ok.gov/OSF/documents/security03012007.pdf](http://www.ok.gov/OSF/documents/security03012007.pdf)

1.4.6 Users shall not represent themselves as others (e.g., log on as another User) unless explicitly authorized to do so. For example, Users shall not:

    1.4.6.1 Send forged e-mail;

    1.4.6.2 Misuse instant messaging systems to disguise the identity;

    1.4.6.3 Log on as another User;

    1.4.6.4 Intercept or monitor network communications intended for another User.

1.4.7 Users shall keep confidential sensitive personal data to which Users have access.

1.4.8 Users shall not solicit on behalf of groups, individuals, or organizations that are not related to OCCC, the OCCC Foundation, or institutionally approved activities.

1.4.9 Users shall adhere to all OCCC Policies and Procedures including, but not limited to, policies on proper use of information resources, information technology, and networks; acquisition, use, and disposal of College-owned computer equipment; use of telecommunications equipment; ethical and legal use of software; and ethical and legal use of administrative data.

1.4.10 Users should be aware that their use of OCCC Information Technology Resources is not completely private. Although OCCC does not condone casual access of Users' electronic files and communications, Users have no expectation of privacy in electronic records stored, accessed or communicated using OCCC Information Technology Resources, including the User's personal communications and personal data stored, accessed or communicated using OCCC Information Technology Resources. Users who wish to maintain the privacy of personal information and communications should store, access and communicate that information or communication using resources not owned or operated by OCCC.

    1.4.10.1 Electronic records and communications created, stored and received in the regular course of OCCC business may be public records subject to disclosure under the Oklahoma Open Records Act.

    1.4.10.2 Electronic records and communications created, stored, accessed, received, or communicated using OCCC Information Technology Resources may be subject to subpoena and/or production in litigation and administrative proceedings.

    1.4.10.3 IITS has the right to monitor the use of OCCC Information Technology Resources and to access, observe, and intercept records and communications in the course of performing network security, operations and maintenance functions or when directed to do so under the authorization described in paragraph 1.4.10.4 below. Any private information accessed in the course of carrying out these responsibilities shall be treated by IITS staff as confidential. However, in the unusual circumstance that an IITS employee detects a violation of policies, procedures, or law while

performing his or her duties operating or maintaining the system, the IITS employee is responsible for reporting the violation to the President's Cabinet member in whose area the violation occurs.

1.4.10.4 Except as otherwise provided in section 1.4.10.3, OCCC reserves the right to access, review, retrieve and inspect records and communications stored on OCCC Information Technology Resources only when such access, review, retrieval and inspection is authorized by the President's Cabinet member in whose area of responsibility the record is created or stored, in consultation with the Vice President for Information and Instructional Technology Services and the General Counsel. Examples of purposes for which OCCC accesses, reviews, retrieves and inspects records and communications include, by way of illustration and not by way of limitation, the following:

1.4.10.4.1 To investigate potential violations of this policy or any other Board of Regents, OCCC, or OneNet policy or procedure;

1.4.10.4.2 To investigate potential violations of federal, state, and local law;

1.4.10.4.3 In health and safety emergencies;

1.4.10.4.4 As necessary to conduct OCCC business, including when the correspondent, creator, or custodian of the record or communication is unavailable;

1.4.10.4.5 In the course of audits, accreditation reviews, and similar procedures; and

1.4.10.4.6 To respond to Open Records Act requests, state agency records requests, subpoenas, and other administrative or judicial records requests.

1.4.11 Any mobile device that contains any confidential OCCC information shall be password protected. This is to include, but is not limited to, personal computers, laptops, email, telephones, cell phones, radios, pagers, or any new portable electronic device or message/communication applications such as texts, twitters, instant messages.

1.4.12 Upon separation from employment, the separating employee's access to OCCC Information Technology Resources will be disabled. Separating employees shall provide to their immediate supervisor all accounts and passwords used on any OCCC Information Technology Resources, including but not limited to Datatel, files, folders, e-mail and voice-mail accounts. The immediate supervisor is responsible for preserving electronic records in accordance with records retention requirements. The immediate supervisor is responsible for notifying Human Resources and IITS of the employee's separation from employment so that access may be disabled in a timely manner.

1.5 Violations of IITS Acceptable Use Policy and/or Terms of Use:

1.5.1 In cases of unauthorized, inappropriate, or irresponsible behavior, OCCC and IITS reserve the right to take immediate remedial action, commencing

with an investigation of the possible abuse. IITS shall have the authority to examine hardware, software, files, passwords, accounting information, printouts, tapes, e-mail, or other material that may aid the investigation. Such examination of User files must be authorized by the President's Cabinet member in whose area of responsibility the behavior occurs, in consultation with the Vice President for Information and Instructional Technology Services and the General Counsel. Users shall cooperate in such investigations. Failure to do so may be grounds for cancellation of access privileges, discipline under the Student Conduct Code or, for employees, discipline up to and including termination of employment.

    1.5.2   Violation of this Policy may result in suspension or revocation of access to OCCC Information Technology Resources and additional discipline, up to and including academic suspension or expulsion, and/or termination of employment. Any action that intentionally interferes with or harms the system or services will be dealt with as a cyber security attack on the OCCC Information Technology Resources and be subject to more stringent penalties.

    1.5.3   Violations may also be referred for civil and/or criminal prosecution under applicable federal, state and local laws.

    1.5.4   Disclaimers:

        1.5.4.1   Other external networks to which OCCC maintains connections (e.g., OneNet, OSRHE and INTERNET) have established acceptable use standards. It is the User's responsibility to adhere to the standards of such networks.

        1.5.4.2   1.5.4.2.   Users of OCCC Information Technology Resources are subject to applicable laws and OCCC policies and procedures. The User assumes all risk of loss of materials or data or damage thereto. OCCC disclaims any responsibility and/or warranties for information and materials residing on non-OCCC systems or available over publicly accessible networks.

        1.5.4.3   1.5.4.3.   Materials residing on non-OCCC systems or available over publicly accessible networks do not necessarily reflect the attitudes, opinions, or values of OCCC, its faculty, staff, or students.

        1.5.4.4   1.5.4.4.   These policies and procedures should not be construed as a limit on any individual's right under the constitution of the United States or the laws of Oklahoma.

2.0   EMPLOYEE EMAIL (e-mail) and VOICEMAIL (v-mail)By using OCCC-owned and provided v-mail, e-mail and Learning Management System (LMS) e-mail services, Users agree to comply with all of OCCC's policies and procedures and local, state and federal laws.

    2.2   In addition to the General Provisions in Paragraph 1 and Terms of Use in Paragraph 1.4 above, the following applies to the use of employee e-mail:

        2.2.1   Assigned e-mail accounts: All OCCC staff, full-time faculty and adjunct faculty shall use official OCCC assigned e-mail or LMS e-mail accounts when conducting official OCCC business by e-mail. OCCC shall presume

that Users have received and read all official OCCC e-mail messages sent to their official OCCC assigned e-mail account(s).

2.2.2   The contents of e-mail are subject to federal and state laws governing public records, records retention, and disclosure of information. External e-mail transmissions may not be secure, and confidential contents shall not be forwarded to a non-OCCC assigned e-mail account. Common examples of confidential contents include: student grades, information derived from educational records, personnel records, medical information, financial information and other records and data subject to the Americans with Disabilities Act (ADA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA), and the Gramm Leach Bliley Act (GLBA). Disclaimers of confidentiality included in e-mail messages do not protect the sender if confidential information is shared or disclosed inappropriately.

2.2.3   In the case of sensitive or confidential messages, the forwarding of official OCCC messages to non-OCCC assigned accounts, including the User's own non-OCCC account, is expressly prohibited. The forwarding of official OCCC messages to non-OCCC assigned accounts is in all cases discouraged.

2.2.4   Employee E-mail and V-Mail Terms of Use: By using OCCC v-mail, e-mail and LMS e-mail services, Users acknowledge and agree to the following:

2.2.4.1   All use must comply with OCCC policies and procedures, as well as federal, state, and local law.

2.2.4.2   All material sent via e-mail or v-mail must be attributable to the individual, organization, or office sending it. Sending e-mail or v-mail in a manner that creates the impression it was sent from another source is a violation of this Policy.

2.2.4.3   Upon separation from employment, the employee shall make all e-mail and v-mail related to OCCC business available to his or her supervisor by providing the supervisor with all passwords. The supervisor is then responsible for storing this information according to OCCC's record retention policy.

2.2.4.4   Upon separation from employment, the employee's employee e-mail and v-mail accounts will be disabled.

2.2.4.5   Only President's Cabinet members and their designees are authorized to utilize the system-created distribution groups. Other users who wish to send emails to system-created groups shall forward the message to their President's Cabinet member or designee for approval.

2.2.4.6   OCCC cannot absolutely protect e-mail or v-mail users from receiving messages that may be offensive to them. Harassing and discriminatory communications should be reported to the EO/AA Compliance Officer in Human Resources.

2.2.4.7   Use shall comply with all College policies and procedures including, but not limited to, this Information Technology

Resources Acceptable Use Policy and OneNet's Acceptable Use Policy.

2.2.4.8 Because mass e-mail consumes large amounts of technological resources, it is an inefficient means of communication. Mass e-mail is also considered spam by many recipients. Therefore, Users may not send mass e-mail of any kind without prior approval of their department head or manager. A mass e-mail is defined as any e-mail or combination of e-mails sent to more than 50 recipients. However, in the case of a mass e-mail directed by a faculty member to students, the e-mail may be sent to no more than 50 students or the total number of students then registered in the sending faculty member's course(s), whichever is greater. Additionally, sponsors and chief officers of faculty organizations and recognized student organizations may exceed the 50-recipient limitation without prior approval when sending announcements related to official organization business.

2.2.4.9 Users shall not send or forward chain letters.

2.2.4.10 Users shall not use OCCC e-mail for buying or selling items. The Pioneer and Electronic Bulletin Board offer traditional and web-based areas to post items for sale or items desired for purchase.

2.2.4.11 In drafting e-mail messages, employees should be aware that communications sent from an e-mail account with an "OCCC.edu" domain name, like communications sent on OCCC letterhead, may be perceived as official communications of OCCC.

2.2.4.12 President's Cabinet, Deans and their appointees may send broad-based messages relating to OCCC business without any prior approval. The author of any college business messages, however, assumes responsibility for assuring that messages do not violate any OCCC policies, regulations, or procedures.

3.0 RETIREE E-MAIL, WEBSPACE AND NETWORK RESOURCE ACCESS

Purpose: Faculty and staff who retire through the Oklahoma Teachers Retirement System directly from employment with OCCC ("Retirees") will be provided with a college e-mail account (username@college.occc.edu). These accounts are provided to facilitate communications with Retirees for purposes of benefits communications, development, promotion, and providing volunteer opportunities at OCCC.

3.1 Assignment of Retiree E-Mail Addresses: IITS will assign each Retiree a new OCCC e-mail address and have it included in a "Retiree" distribution list. It is to this address that OCCC will send e-mail communications. A Retiree may have OCCC e-mail electronically redirected to another e-mail address.

3.2 Retiree E-Mail Terms of Use: Users of Retiree e-mail are subject to the Terms of Use set forth in Paragraph 1.4 under General Provisions above. Users of Retiree e-mail acknowledge and agree that:

3.2.1 All use of Retiree e-mail must comply with OCCC policies and procedures, OneNet's Acceptable Use Policy, and federal, state and local law.

3.2.2 All e-mail sent using the OCCC system must be attributable to the individual sending it. Sending e-mail in a manner that creates the impression that it was sent from another source is a violation of this policy.

3.2.3 OCCC cannot protect e-mail users from receiving messages that may be offensive to them. Harassing and discriminatory communications must be reported to OCCC's EO/AA Compliance Officer.

3.2.4 IITS will delete Retiree e-mail accounts that have been dormant for 18 months.

3.3 General Account Information: This account comes with several changes that make it different from the previous college assigned e-mail account. Below is a list of those changes.

3.3.1 The e-mail box size is reduced to a 25MB size limit. Retirees must actively manage the e-mail account to prevent the size from exceeding the 25MB limit. Messages will be returned as undeliverable if sent to a Retiree e-mail box that exceeds 25MB limit. IITS will provide assistance with moving existing e-mail from employee e-mail to the new e-mail account.

3.3.2 Retirees do not receive e-mail addressed to "All Campus" or "All Employees". Communications to retirees must be addressed to retirees individually or, when authorized, by using the Retirees distribution list.

3.3.3 All Retirees belong to the organizational group "Retirees." Retirees will not receive departmental e-mail from the last department of employ unless the e-mail is specifically addressed to the individual Retiree.

3.3.4 IITS will provide technical support to configure the connection to the new e-mail address, but will not troubleshoot Retiree personal computers.

3.4 Webspace provided during employment is not available to Retirees. IITS will provide assistance with backing up this information for use later.

3.5 Network Resources: Access to shared network resources is not available to Retirees. This includes any content on the "I:" drive, as well as Group shares.

3.6 Dialin privileges are not available to Retirees.

4.0 STUDENT E-MAIL

4.1 Purpose and Scope of Policy

4.1.1 Due to the increasing reliance and acceptance of electronic communication, e-mail is considered an official means for communication within the OCCC community.

4.1.2 Scope: This student e-mail policy provides guidelines regarding the following aspects of e-mail as an official means of communication:

4.1.2.1 College use of e-mail;

4.1.2.2 Assignment of student e-mail addresses;

4.1.2.3 Student use of and responsibilities associated with assigned e-mail addresses;

4.1.2.4 Expectations of e-mail communication between faculty and

4.2 Assignment of Student E-mail Addresses: IITS assigns each student an official OCCC e-mail address. It is to this official address that OCCC will send e-mail communications. This official assigned e-mail address will be the address recorded in the Student Information System.

4.3 Student Responsibilities:

4.3.1   Official Means of Communication: Because e-mail is an official means for communication within OCCC, OCCC has the right to send communications to students via e-mail and the right to expect that students shall open and read e-mail in a timely fashion.

4.3.2   Redirecting E-mail: A student may have e-mail directed to his or her official OCCC e-mail address electronically redirected to another e-mail address at his or her own risk. If a student wishes to have e-mail redirected from his or her official address to another e-mail address (e.g., @aol.com, @hotmail.com, or other e-mail server), they may do so. However, OCCC will not be responsible for the handling of e-mail by outside vendors and compliance with FERPA no longer pertains. Redirecting e-mail does not absolve a student from the responsibilities associated with communications sent to his or her official e-mail address.

4.3.3   Checking E-mail: Students are expected to check their official e-mail address on a frequent and consistent basis in order to stay current with OCCC communications. OCCC recommends checking e-mail once a week at a minimum in recognition that certain communications may be time-critical.

4.4   Educational Uses of E-mail: Faculty shall determine how e-mail will be used in their classes. Faculty who have e-mail requirements and expectations shall specify these requirements in their course syllabus. Faculty have the right to expect that students' official e-mail addresses are being accessed, and faculty may use e-mail for their courses accordingly.

4.5   Appropriate Use of Student E-mail:

4.5.1   In general, e-mail is not appropriate for transmitting sensitive or confidential information unless its use for such purposes is matched by an appropriate level of security.

4.5.2   Confidentiality regarding student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of e-mail, including use for sensitive or confidential information, must be consistent with FERPA.

4.5.3   E-mail shall not be the sole method for notification of any legal action.

4.6   Student E-mail Terms of Use: In addition to the General Provisions in Paragraph 1 and Terms of Use in Paragraph 1.4 above, Users of student e-mail acknowledge and agree that:

4.6.1   All use of student e-mail must comply with Student Conduct Code, OCCC policies and procedures, and federal, state and local law.

4.6.2   All material sent via e-mail must be attributable to the individual, organization or office sending it. Sending e-mail in a manner that creates the impression it was sent from another source is a violation of this policy.

4.6.3   OCCC cannot protect e-mail users from receiving e-mail that may be offensive to them. Harassing and discriminatory communications must be reported to the EO/AA Compliance Officer.

4.6.4   Use must comply with all OCCC policies and procedures, including, but not limited to, the Information Technology Resources Acceptable Use Policy and OneNet's Acceptable Use Policy.

5.0   OCCC WIRELESS NETWORK
    5.1   Purpose and Scope:
        5.1.1   The OCCC wireless network ("WLAN"or "WI-FI") is intended to be a convenient supplement to the wired network for general functions, including web browsing and use of e-mail. Wireless "access points" located throughout the campus allow suitably equipped and configured devices to make wireless connections to the OCCC network, including the Internet. The OCCC WLAN is designed to support a wide-range of WI-FI (802.11a, 802.11b, and 802.11g, etc.) equipped computers, notebooks, PDAs, and other devices.

    5.2   Use Limitations
        5.2.1   WLAN performance deteriorates as the number of users and traffic increases. Distance from the access point, buildings or objects shielding the access point, signal interference, quality of equipment, battery power and other factors may also impact performance. As such, the wireless network should not be expected to provide the same quality-of-service as the wired network. When reliability and performance are a must, the wired network should be used.

        5.2.2   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. In addition, wireless networks are highly sensitive to overlapping frequencies and can present a risk to the integrity and security of the OCCC data network. To promote efficient and secure wireless network access, Information and Instructional Technology Services (IITS) maintains strict standards for the deployment of wireless devices at OCCC.

        5.2.3   Security hardware and software will disconnect you temporarily or permanently from the entire OCCC network if you attempt to circumvent standard procedures and protocols, or attempt to access or manipulate equipment which you are not authorized to access. Such attempts also subject the User to penalties under Paragraph 1.5 of this Policy.

    5.3   Terms of Use: Use of OCCC wireless service is governed by this IITS Acceptable Use Policy (No. 3058). In addition to the General Provisions in Paragraph 1. and Terms of Use in section 1.4 above, by accessing or attempting to access the OCCC Wireless Network, Users acknowledge and agree to the following:

        5.3.1   Users must submit all wireless access points to IITS for approval and registration before they are connected to the OCCC network.

        5.3.2   Broadcast frequencies used by the wireless networks may be monitored on OCCC property. Devices that generate interference with the OCCC wireless network are subject to restriction or removal.

        5.3.3   Other than "guest" access, only authenticated access to OCCC's wireless network is permitted. Typically, authentication and access is provided from a series of logon screens and logs may be used for assessing network problems or identifying unauthorized or unacceptable use of the wireless network.

        5.3.4   All college owned WI-FI devices must be registered with IITS before they are used.

5.3.5   IITS will configure OCCC owned faculty and staff wireless devices with WI-FI access software suitable for authentication and encryption when they are registered with IITS. Wireless configuration settings made by IITS shall not be changed. Doing so could introduce serious security vulnerability.

5.3.6   The wireless network's maximum data speed is lower than the speed of OCCC's wired network. High bandwidth operations, such as large file transfers and media sharing with peer-to-peer programs (i.e., KaZaa, Gnutella, or Bearshare) do not constitute acceptable use of the wireless network.

5.3.7   Performance varies and cannot be guaranteed.

5.3.8   Off-campus connections to the wireless network are not permitted.

5.3.9   Devices connecting to the wireless network must be capable of meeting minimum security standards, as defined by IITS. Some older devices do not meet these standards, and may not be used on the wireless network.

5.3.10   A "guest" wireless connection is available for persons who visit OCCC for brief periods of time. Guests may receive an access code by providing identification and, where required, proof of age and registering with appropriate OCCC staff.

5.3.11   The OCCC WLAN is as secure as any open public access network, like public telephones and dial-up Internet accounts. Users are advised that confidential data should be sent or received only on SSL-encrypted web pages.

5.4   Restrictions on On-Campus Wireless Access Points Not Owned by OCCC.

5.4.1   The use of non-IITS-provided wireless access points, connected to the OCCC network, poses a security risk that could give unauthorized or malicious persons access to confidential OCCC data. It can also degrade the performance of OCCC-provided wireless services. Because of these risks, OCCC restricts the use of wireless access points connected to the OCCC network. Only IITS-provided or approved access points are permitted. Specific details are outlined below.

     5.4.1.1   Students: Student-owned access points may not be used on college property. Peer-to-peer programs (i.e. KaZaa, Gnutella, or Bearshare) are not permitted. Students wishing to wirelessly connect to the OCCC network must use IITS-provided (and secured) wireless access points.

     5.4.1.2   Faculty & Staff: Because they often handle confidential OCCC data, faculty and staff wishing to use OCCC-owned or personally owned wireless devices must use IITS-provided (and secured) SSID connections.

     5.4.1.3   Enabling Windows Internet Connection Sharing and similar features effectively turns a laptop into an access point. In order to avoid interference with the OCCC-provided wireless networks, these features must be disabled while the wireless device is used on OCCC property.

Effective Date: 07-01-96

Revised Date: 02-05-07
Revised Date: 09-21-09
Revised Date: 05-17-10
Revised Date: 06-27-11