IT Policies for Students

By using the technology provided at North Greenville University, you agree to abide by the following policies for acceptable use.

Network Acceptable Use

The NGU network must not be used for any activity that does not support the mission and purposes of North Greenville University. If a particular usage is not in the best interest of the University, or if it does not support the University's mission and purposes, then it must not be performed. 1. Deliberate disruption of NGU technology resources is expressly prohibited, including any action intended to disrupt system services, user accounts, network performance, Internet access or any other technology resources. 2. Students must not make any unauthorized copies of copyrighted materials, (software, media, etc.). Software provided by NGU is purchased under software licensing agreements that place legal restrictions on their use and copying. 3. The NGU network must not be used for any unlawful or malicious purposes. Specifically, resources must not be used by anyone to transmit threatening, obscene, harassing, or pornographic materials, or any outcome that would interrupt the normal operations of provided services. Any attempts to penetrate remote or local service without proper authorization are forbidden. 4. Students must not intentionally seek information about, browse, copy, or modify files or passwords belonging to other students. Students must not attempt to decrypt or translate encrypted material not intended for them or obtain system privileges to which they are not entitled. If a network security exposure is encountered or observed, it must be reported to Information Technology Services (ITS) immediately. 5. The use of p2p (peer-to-peer) "file sharing" applications is prohibited. First, Copyright infringement is illegal and subject to federal and civil prosecution. Second, a large percentage of files being downloaded are indecent, obscene, and a violation of the University's mission and purpose as a Christian institution. Third, the excessive traffic generated by file sharing applications is wasteful of network resources, causing significant problems for all network users. 6. Students are prohibited from attaching any wired or wireless "network device" to any campus network connection that functions as a bridge or routing device. Such network devices include routers, switches, bridges, access points, and any printer or streaming device that functions as a bridge or router. With the exception of end-point wired hubs, wireless printers, or wireless streaming devices (which students may install in their rooms as needed), the installation and configuration of any network devices on the University's network is solely the responsibility of the ITS department. 7. Students may not run any network services (e.g., DHCP, DNS, WINS, FTP, NAT, etc.) via any kind of file server or web server or host any Internet-based services on a computer or laptop. 8. Students may not circumvent firewall or Internet filtering functions by using tunneling or proxy server techniques. 9. The University provides wireless service across campus, including all computer labs, classrooms, and residential buildings. If anyone other than an authorized employee installs an unauthorized or unregistered device on the campus network, such device will be confiscated and the offender will face applicable disciplinary sanctions. 10. Students must not create or willfully disseminate computer viruses. Students must install anti-virus software on their desktops or laptops and must take adequate steps to ensure that virus signature/update files are maintained and updated regularly. 11. Students must regularly (at least once a month) apply operating system patches as provided by the OS vendor (Apple, Microsoft). Assistance in applying OS patches can be obtained from the ITS Helpdesk. 12. Students need to be aware that there are federal, state, and sometimes local laws that govern certain aspects of computer and telecommunications use. Students are expected to respect these laws and to observe and respect

University rules and regulations. 13. Any questionable use must be considered “not acceptable.” In cases where it may be necessary to request an exception to any of these policies, such requests must be submitted in advance to the ITS Department for review and possible approval.

E-Mail Acceptable Use Policy E-mail services are provided by NGU and should be used to support the mission and purposes of the University.

1. E-mail services may be used for incidental personal purposes provided such use: a. Does not directly or indirectly interfere with the operations or e-mail services of the University b. Does not burden the University with noticeable incremental cost c. Does not interfere with the e-mail user’s employment or other obligations to the University.

2. Students are not permitted to send e-mail solicitations and must not forward e-mail chain letters to any person, on or off campus, except to forward a message to the ITS Department. 3. Only authorized employees may send broadcast e-mail messages. Unauthorized users are specifically prohibited from using the University’s Address Book to harvest e-mail addresses for bulk e-mail purposes. Requests to send broadcast e-mail messages may be submitted to Student Life. 4. Students should be aware of the following: a. E-mail is less private than users may anticipate. b. Deleted e-mail may persist on backup facilities and thus be subject to disclosure under state and federal law. c. E-mail stored on University equipment, whether or not created on University equipment, constitutes a University record subject to disclosure. d. The University cannot protect users from receiving all e-mails they may find offensive. e. Students are strongly encouraged to use the same personal and professional courtesies and considerations in e-mail as they would in other forms of communication.

Internet Acceptable Use

Policies High-speed Internet services are provided by NGU and should be used to support the mission and purposes of the university. 1. Web site filtering is performed to block Internet sites that are offensive, malicious, bandwidth intensive, illegal or unethical. Web sites in categories that will be blocked include but are not limited to the following: adult content, gambling, hacking, audio/video streaming, pornography, tastelessness, sexuality and violence. 2. It is a violation of the Internet Acceptable Use Policy for any student to bypass or attempt to bypass the Web content filtering controls used on the NGU network. 3. If a particular website is blocked and a student needs access to this site as part of their approved academic purposes, a request to unblock the site must be sent to the ITS Helpdesk by the student’s professor. Requests will be considered on a case-by-case basis. 4. The CIO will review the request and ultimate approval to unblock a site will come from the Vice President for Academics.

Cellular and Mobility Acceptable Use Policy

Cell phones and other communication devices are permitted for personal use. Cell phones must be used in the silent/buzz mode whenever a student is in attendance in the classroom, chapel, cultural events, or other school directed requirements for attendance. If the device does not have the silent/buzz mode,

the device should be turned off. While in class, chapel or cultural events phones should remain in your pocket or purse unless otherwise instructed by a faculty or staff member. Students may not use phones for calls, text messaging, games or other uses during class, chapel or cultural events. Students may use smart phones, electronic notebooks, and other similar devices if they are using them as their Bible. Faculty may impose standards for use in addition to this policy.

Students agree to refrain from using cellular devices with “Hotspot” functionality on campus. These devices and associated technology should not be used to circumvent any decency or acceptable use standards for all students, faculty, and staff whether on campus or away.