Gardner-Webb University
Technology and Acceptable Use Policies

The purpose of this policy is to describe the appropriate use and security of University Technological assets, associated responsibilities, and rights of all Users employing these resources. All Users of University Technology assets are expected to be familiar with each policy contained here within and the consequences of violation as listed below. This policy supersedes all previous Gardner-Webb University Computer Usage Policies.

Violation of these contained policies may result in the immediate suspension of computer account and network access pending investigation resolution. Depending on frequency and/or severity, the offender may lose all computer account and network access in addition to facing the appropriate University judicial review. The penalties may include suspension or dismissal from the University and/or criminal prosecution where warranted.

Network Security and Privacy Policies:

1. Unauthorized attempts to gain privileged access or access to any account or system not belonging to you on any University system are expressly prohibited.
2. Creation of any program, Web form, and/or any other mechanism designed to gain privileged account information is prohibited without the written permission of the Provost and Associate Vice President for Technology Services.
3. Computer and network accounts are assigned to each individual uniquely and are considered confidential in nature. Individual accounts cannot be transferred to or used by another person. Given that access allows the User to retrieve personal information of the individual assigned the account, sharing of accounts and/or passwords is not permitted.
4. Each User is personally responsible for the proper use of his/her account including all activity associated with his/her account. All illicit activity that can be traced to a User account will result in immediate termination of the account until the investigation is complete. Users who do not safeguard their Usernames and passwords may lose their access permanently, subject to the appropriate University judicial review.
5. Each system owner is responsible for the security of all systems he/she connects to the campus network (WebbNet). Any system determined to cause network degradation and/or attacks other systems as a result of malicious software, e.g. viruses, worms, Trojans, will be removed from the network immediately and without notification until the system has been made secure.
6. No University-owned or private system attached to the WebbNet may be used as a vehicle to gain unauthorized access to any other system whether on or off campus.

7. The storing of sensitive personal information belonging to any Gardner-Webb customer, vendor or system user such as social security numbers, credit card information or any kind of known sensitive personal data in a cloud account or on a desktop computer, laptop computer, flash drive, DVD or any other media is strictly prohibited.
8. Anyone believing that a possible security lapse has occurred on any University technological resource or network MUST report it immediately to the respective department chairperson/manager and to Technology Services. The system and/or computer associated with the lapse should not be used until the problem has been investigated and cleared by the system administrator.
9. All Users must be aware that Gardner-Webb system administrators conduct periodic security checks of University systems and networks. Additionally, outside agencies are annually contracted to assess and challenge the University systems and network security to ensure a safe operating environment. As a result of the analysis, Users may be required to change their passwords during their next log-in process where an easily guessed password has been employed.
10. User files on a University server/system are kept as private as possible. Any attempts to access and/or read another person's protected files will be treated with the utmost seriousness. System administrators will not override any file protections unless deemed absolutely necessary in the performance of their duties and will treat the contents of those files as private and confidential information at all times. System administrators must make every effort to communicate with the owner of the files in the event any file protection is overridden.
11. Faculty and staff computers are required to have a screen saver set that will lock a computer after 15 minutes of inactivity. This setting is set by Technology Services, when a computer is installed for an employee. However, occasionally Windows' updates or other factors may alter the screen saver setting. Should you find your screen saver is not activating and locking your computer after 15 minutes of inactivity, update the following settings.

Windows 10:

1. Type **Lock Screen Settings** in the Search box in the lower left corner of your screen. Select **Lock Screen Settings** in the results displayed.
2. In the right pane, select **Screen saver settings**.
3. Set the value in the **minutes** box to 15. Check the box beside **On resume, display logon screen**.
4. Change the **Screen saver type**, if desired.
5. Click **OK** and close the Settings window.

Mac OS 10.13-10.15:

1. From the Apple menu, select **System Preferences**.
2. Select **Security and Privacy**

3. On the **General** tab, check the box beside **Require password** and set the minutes to 15.
4. Close the window when finished

Password Policies:

1. Passwords are personal in nature and should not be shared with anyone other than Technology Services working with you to resolve an issue. Once the issue has been resolved it is recommended that the user change their password.
2. Passwords must be changed every 180 days for current students, faculty, adjuncts, and staff. You will be notified via email at 15 days from expiration and then on days 10,5,4,3,2,1 to update your password. Once you update your password the 180-day cycle starts again.
3. If your password does expire, you will no longer have access to any university system. This include desktops/laptops, wireless, WebbConnect, Blackboard, etc. You can use the Forgot Password link on the WebbConnect login page to reset your password once expired.
4. The new password must meet the minimum requirements set forth in our policies:
    a. It must be at least 8 characters long
    b. It must contain, at minimum, 3 of the following:
        i. Uppercase letters (A-Z)
        ii. Lowercase letters (a-z)
        iii. Numbers (0-9)
        iv. Symbols (!@#$%^&*...)

    c. It cannot match any of your past 10 passwords
    d. It cannot contain 3 consecutive characters of your username
    e. You cannot change your password more than once in 24 hours

5. For wireless/mobile devices, you will need to “forget” the GWUWireless wi-fi and reconnect using your new credentials after a password change.

6. For employees with a university-issued laptop, you will need to have the laptop on campus to update the computer's logon password.

Network and Computing Usage Policies:

1. No University system or network may be employed in a manner or purpose that violates University statutes/regulations/policies and/or federal, state or local laws.
2. Any activity, malicious or otherwise, resulting in obstructing the operation and work activities that employ University technological resources will not be

tolerated. Activities include, but are not limited to, consuming gratuitously large amounts of system resources (disk space, CPU time, network bandwidth), and/or crashing University servers or individual machines.

3. Use or access of any University system by outside persons or agencies requires written permission from the Provost Office and Technology Services to include payment of fees to the University and appropriate software vendors where applicable.
4. Use of University technological resources, systems, and networks for commercial purposes is strictly prohibited except where explicitly approved by the Provost. Such prohibited use includes, but is not limited to, development of programs for commercial profit, data processing or computations for commercial use, and preparation/presentation of for-profit advertising material. Posting of published works, workshops, presentations, etc., related to a faculty member's area of teaching are exempt from this prohibition.
5. Frivolous, disruptive, and/or inconsiderate conduct including the access or use of pornography in any University computer lab, multi-media, or other room including any office which employs technology is not permitted.
6. No University computing facility may be used for participating in computer gaming outside of academic requirements.
7. Copying, storing, displaying, or distributing copyrighted material using University systems and/or networks without express permission of the copyright owner, except as otherwise allowed under copyright legislation, is strictly prohibited. Under the Digital Millennium Copyright Act of 1998, repeat copyright infringements by a User can result in termination of the User's access to University systems and networks. Statutory damages for copyright infringements range from $750 to $30,000 per infringement with willful infringements carrying potential damages up to $150,000 plus attorney fees.
8. Tampering, reconfiguring, equipment removal, and physically accessing University network/computing resources and/or wiring without express permission by Technology Services or Plant Operations is strictly prohibited. Such action will be considered vandalism and/or theft and will be prosecuted to the fullest extent of University policy and criminal law.

E-Mail Usage Policies:

1. Gardner-Webb University has established e-mail as a primary vehicle for official communications with enrolled students and current faculty/staff.
2. Every enrolled student, and current faculty and staff member has an official Gardner-Webb University e-mail address established and assigned by Technology Services. **All University communications sent via e-mail will be sent to and from this address. Faculty members will use the official University e-mail address to communicate with a student registered in their classes. Additionally, all students, faculty, adjuncts, and staff are**

required to use their assigned Gardner-Webb email address for any and all university communications.

3. Students are expected to check their official e-mail address on a frequent and consistent basis in order to stay current with University communications. A student's failure to receive and read University communications delivered to his/her e-mail address in a timely manner does not absolve the student from knowing and complying with the content and instructions of such communications.
4. Students are allowed to forward their e-mail from their official University e-mail address to another provider but do so at their own risk. Gardner-Webb is not responsible for the handling of e-mail of other service providers. Having e-mail forwarded does not absolve students from knowing and complying with the content of communications sent to their official University e-mail address.
5. No e-mail may be sent or forwarded through a University system or network for purposes that violate University statutes and/or regulations and constitutes an illegal or criminal action.
6. Electronic mail is considered private, confidential information and will be kept as private as possible. Attempts to read another person's e-mail will be treated with the utmost seriousness. No University employee or system administrator will read any mail unless deemed absolutely necessary in accordance with specific job requirements or by judicial subpoena. The University makes every effort to respect e-mail privacy and adhere to state and federal statues governing e-mail confidentiality. However, the University reserves the right to investigate virus and illicit activity that can be introduced through e-mail systems. Additionally, if requested by the person assigned to the e-mail account, Technology Services may enter the specific e-mail account to assist with problem identification and resolution.
7. Users should be aware that deletion of electronic information will not erase such information from the system storage until overwritten with other data. This can result in the information residing in the University's network either on various back-up systems/media until such time as the information is overwritten.
8. Nuisance e-mail or other on-line messages such as chain letters, obscene, harassing, and/or other unwelcome messages are prohibited.
9. Unsolicited e-mail messages to multiple Users are prohibited unless explicitly used for University instruction and/or business purposes. Exceptions are granted by the appropriate University authority.
10. All messages must show accurately from where and from whom the message originated, except in cases where anonymous messages are invited.
11. Gardner-Webb reserves the right to refuse mail and other communications from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain virus and/or illicit material. The University will refuse, filter and/or disregard such messages.

12. The email/WebbConnect account will be deleted no later than 5:00 pm the day of the employee's separation from the university. An email/WebbConnect account may remain active for a specified period of time upon the written request of the employee's supervisor and the approval of the appropriate vice president or associate provost. The password for the account will be changed so the employee no longer has access to the account. Requests should be submitted to the Associate Vice-President of Technology Services.
13. Terminated employees who are current or former students will retain a Gardner-Webb University email address.
14. Retiring faculty may request their account remain active indefinitely; these requests should also be submitted in writing to the Associate Vice-President of Technology Services and will be subject to approval by the Provost.

Gardner-Webb Electronic Academic Code:

This principle applies to works of all authors and publishers in all media. Respect for intellectual creativity and work is vital to academic discourse and enterprise. It encompasses respect for the right to acknowledgment, the right to privacy, and rights to determine the form, manner, and terms of publication and distribution.

Due to the volatility and ease of reproduction of electronic information, respect for the work and personal expression of others is especially critical in computing environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secrets and copyright violations may lead to serious consequences as deemed appropriate by respective University judicial review panels.

User Responsibilities:

Users of University technological resources, systems, and/or networks are responsible for what they do on the network. Any illicit activity will be taken very seriously. Each User must maintain a current version of antivirus software and stay current with any operating systems patch releases. The University employs software to ensure that all computers accessing the network are compliant with this requirement, forcing Users to update to the current applicable versions before allowing them to connect to the University network.

Users must respect and adhere to all University policies and federal, state, and local laws to include, but not limited to, copyrights, intellectual property rights, and confidential information access. It is a violation of Gardner-Webb policy to copy, distribute, share, download or update any copyrighted material without the express permission of the copyright owner.

Users must respect network access and bandwidth requirements. Any User determined to be consuming excessive bandwidth that negatively impacts the performance of University systems, users, and/or networks may be disconnected from the network without warning.