Waynesburg University
Network Policies for Residence Hall Network

1. You are personally responsible for the use of your computer and will be held accountable for any violations that occur involving your computer. Additionally, you are responsible for what your roommate(s) or friends do with your computer.

2. Your computer must meet Comcast's documented minimum requirements in order to be supported by their Service Team.

3. Comcast requires that each student read and comply with their "Acceptable Use Policy" (AUP) for Internet activity. Link to AUP: http://www.comcast.net/terms/use

4. You must practice proper maintenance of your computer to ensure it has the capacity to run efficiently on the Residence Hall Network (wired and wireless network).

5. You must have an Anti-virus and Anti-spyware software product installed on your computer and it is your responsibility to keep them up to date. Neither the University, nor Comcast, are responsible if a student computer gets infected by another student computer or from outside sources on the Internet.

6. You must update and patch your operating system, as your O/S vendor makes critical updates available.

7. The use of any IP address or modification to the network configuration other than what is assigned by the University is prohibited.

8. Tampering with the cable modem, network jacks, connected wiring, or any wiring and equipment in your room or Residence Hall lobbies or wiring closets is prohibited.

9. Connection of your personal computer to Academic and Administrative buildings through wired or wireless means without adhering to the above policies is prohibited.

10. Lab computers are not part of the Resnet and are to be primarily used for educational purposes. The use of Lab computers for playing software games should be limited to periods of time when there is less demand for Lab resources. The playing of software games is not allowed if it negatively affects the performance of the network or is disruptive to the Lab environment.

11. The use of University network resources, including Internet access, for illegal or unethical activities is prohibited, which includes, but is not limited to, using computers in a way that causes harassment or the display of false system messages, attempting denial-of-service attacks, degrading or restricting network access for others, exploiting security holes, circumventing security, or in any way gaining unauthorized access to any computing resources.

12. Users will be held responsible for the postings they make (electronic or otherwise), both on and off campus. All postings made to news groups, weblogs (blogs), etc, either on or off campus, must include identification information about the individual who made the posting. Anonymous posting or postings using a pseudonym are not permitted. Postings that are made in the name of another individual other than the author are considered forgeries and are against University policy.

13. Care should be taken when posting information in Social Directories, such as Facebook, MySpace, etc. In these situations, identification information should be kept to a minimum

Revised Date: 7/19/10
Approved Date: 7/19/10
Approved By: Peter E. Mahoney   **Refer to the University Network Policy for more comprehensive information**

and users should be very careful about the type of personal information that is being displayed and shared with others. Make sure the image you project on-line is one that accurately represents you and that you protect yourself by taking advantage of the privacy settings, which help control who can access your information.

14. Any action, whether intentional or unintentional, that affects the performance of the network may result in disconnection until the problem is rectified.

15. The receipt, transmission, or use of software, data, or other intellectual property must observe <u>ALL</u> copyright laws, license restrictions, and policies. The University will fully comply with any investigations of violations and those responsible for such abuse will be held legally accountable.

16. Comcast and the University have the right to monitor residence hall or wireless bandwidth consumption at any time and to limit or prohibit excessive bandwidth consumption.

17. The operation of any server related applications or devices is prohibited, which includes, but is not limited to Web servers, Email servers, FTP servers, News servers, LAN servers, file sharing applications, establishing domain names, and the promotion of a commercial business in any form.

18. The connection of any network device to the network jacks other than a network card attached to a personal computer or a game console is prohibited, which includes, but is not limited to routers, switches, gateways, wireless access points, bridges, and repeaters. Only one device is allowed per network jack in a room.

19. You should be aware that the Resnet and wireless network, including all data files, software applications, E-mail, and Internet access, are University property and are intended to be used primarily for education-related communication and activities. Comcast and the University reserve the right to monitor, access, read and delete any electronic communication that is created, received or sent over its network. Comcast and the University reserve the right to access, disclose and monitor network use at any time without further notice.

20. Network service may be intentionally interrupted from time to time for maintenance purposes. Unintentional interruptions may occur and the University, along with Comcast, will work to restore service as quickly as possible. Comcast and the University are not responsible for any losses or damages caused by service interruptions or other failures of network equipment.

21. These policies will be strictly enforced. Comcast and the University reserve the right to disconnect users at any time for violation of the above policies or Comcast's AUP.

22. Failure to comply with any of the above terms or Comcast's AUP may result in the suspension of computer use privileges and disciplinary review under the appropriate procedures (Student Handbook).

These policies are NOT exhaustive, but rather provide the essential framework for acceptable use of the computer and communication resources of Waynesburg University.

Revised Date: 7/19/10   2
Approved Date: 7/19/10
Approved By: Peter E. Mahoney **Refer to the University Network Policy for more comprehensive information**