STUDENT NETWORK AND INTERNET
ACCEPTABLE USE POLICY AND AGREEMENT

Dear Parents:
Many times throughout the summer instructors will utilize campus computer labs to enhance your child's learning. In order to use these labs, parents must sign the WSU network and Internet policy below. If you have any questions please contact the Pre-College Office at 775-3135.

Wright State University (the "University") is pleased to make available access to interconnected systems within our campus and to the Internet for the purpose of productivity, research, curriculum delivery, professional development activities and electronic storage in the pursuit of learning. The University has policies, which govern the access and use of computer and network systems. This Acceptable Use Policy and Agreement ("Policy") is a guideline for use and a contractual agreement between the student and the University. All students must take responsibility for appropriate and lawful use of their access. Misuse under the guidelines of this document may result in disciplinary action under University Policy and/or the governing code of conduct.

Upon review and signing of this Policy, each student will be given the opportunity to enjoy access to the Wright State University computer and network systems and is agreeing to follow this Policy.

I. Personal Responsibility.

You agree not only to follow the rules in this Policy, but also agree to report any misuse of the network. Misuse means any violation of this Policy, University Policy or any other use that is not included in such policies, but has the effect of harming another person or his or her property.

II. Terms of Permitted Use.

Technology and the Internet are integral components of a quality education. They are no longer optional instructional resources. It is the expectation that all students have access to technology and the Internet and conduct such use in a responsible manner.

By signing this Policy, students acknowledge and understand the following regarding the use of the University computer/network:

1. Electronic mail (e-mail) is not private. Systems managers have access to all messages relating to or in support of illegal activities, activities not in the best interest of the University, and such activities may be reported to the authorities.

2. All electronic data that passes through a University owned computer or over the University's network is subject to monitoring and seizure and may be handed over to law enforcement officers.

3**.** All electronic data created for administrative or instructional purposes for a course or program is the property of the University.

4. The rules and regulations of on-line etiquette are subject to change by the University Administration.

5. The user in whose name a computer account is issued is responsible for Its proper use at all times. Users must log off the computer to conclude a session or lock the computer if stepping away. Users retain responsibility for the activity of anyone accessing the computer and/or network under their account. Users shall keep personal account information, home addresses and telephone numbers private. They shall use this system only under the login and password information issued to them by the University. Users shall not grant others access to a computer and/or the network under their login and password.

6. Computer systems and the University network shall be used only for purposes related to education.

7. Violation of this Policy may result in the cancellation of user privileges and possible discipline under the student code of conduct.

III.   Purpose and Use.

A. Acceptable Use
Wright State University is providing access to its computer network and the Internet for educational purposes only. If you have doubt about whether a contemplated activity is educational, you should ask your professor or instructor if a use is appropriate.

B. Unacceptable Use

The uses that are considered unacceptable include (but are not limited to) the following:
1. Violating or encouraging others to violate the law or University Policy. 2. Revealing private information about yourself or others. Private information includes, but is not limited to a person's password, social security number, credit card number or other confidential information that has the potential to harm yourself or others or to violate the law if shared with other persons.
3. Uses that cause harm to others or that cause damage to their property.
4. Uses that constitute defamation (i.e. harming another's reputation by lies), or that harass, threaten or bully others.
5. Using profanity, obscenity or other language, which may be offensive to other users.
6. Uses that are for commercial transactions (i.e. buying or selling or making arrangements to buy or sell over the internet).
7. Use that causes disruption to the use of the computer and/or network by others or that disrupts the educational process of the University.
8. Using the system to encourage the use of drugs, alcohol or tobacco
9. Viewing, downloading or transmitting material that is threatening, pornographic, obscene, disruptive or sexually explicit or that could be construed as harassment or disparagement of others based on their race, national origin, citizenship status, gender, sexual orientation, age, disability, religion or political beliefs.
10. Copying or placing copyrighted material or software on the system without the author's permission and/or in violation of law.
11. Reading, deleting, copying or modifying other user's email or files without their permission or attempting to interfere with another user's ability to send or receive electronic mail.

Over

12. Using another person's password or some other identifier that misleads recipients into believing someone other than you is communicating or accessing the network or Internet.

13. "Hacking," gaining, or attempting to gain unauthorized access to computers, servers, computer systems, internal networks, or external networks.

14. Downloading and/or installing freeware or shareware programs without the approval of the University Computing Services Department.

15. Uploading a worm, virus or other harmful form of programming onto the network or Internet.

16. Plagiarizing copyrighted or non-copyrighted materials for personal gain, recognition, or as graded work.

17. Using, installing, or attempting to install peer-to-peer file sharing programs such as Kazaa, Bittorent, Limewire, Bearshare, and others.

18. Using social network sites such as MySpace, Xanga, and others and/or forum sites and/or blog sites for the purpose of posting slanderous or otherwise harmful information, whether true or untrue, about the character and/or actions of the University's students or staff on University or personal technology equipment.

19. Using instant messaging, text messaging, and Internet telephony services without the consent of your professor or instructor.

C.   Network and Internet Safety

When using the University's network or Internet, do not reveal personal information about yourself such as your home address or telephone number. Do not arrange a face-to-face meeting with someone you "meet" on the computer network or Internet without your parents' permission.

I understand that Wright State University does not utilize content filtering and that some materials on the Internet may be objectionable; therefore I agree to accept responsibility for guiding my child and conveying to her/him appropriate standards for selecting, exploring, and/or sharing information and media. I realize the University would not be able to provide access to these resources if it had to accept liability for a minor's activities. In exchange for the opportunity for my minor child to participate, I agree to hold the University harmless against any harm that I or my minor child may suffer against a result of this unrestricted access.

IV.   Privacy.

Wright State University reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of Wright State University and no user shall have any expectation of privacy regarding such materials.

V.   Warranties/Indemnification.

Wright State University makes no warranties of any kind, either express or implied, in the connection with its provision of access to and use of its computer networks and the Internet provided under this Policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Policy. Users take full responsibility of his or her usage and agree to indemnify and hold harmless Wright State University and its Board members, administrators, professors, teachers and staff from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agrees to cooperate with Wright State University in the event of the initiation an investigation into a user's use or his or her access to its computer network and Internet, whether that use is on a University computer or on another's outside Wright State University's Network.

****

VI.   Acknowledgment.

I have read, understand and agree to abide by the terms of the foregoing Acceptable Use Policy and Agreement. Should I commit any violation or in any way misuse my access to the University's computers, computer network, and / or Internet, I understand and agree that my access privilege may be revoked and disciplinary action may be taken against me as outlined in the applicable University Code of Conduct.

Over