### The Campus’s Current Acceptable Use Policy

#### Acceptable Use Guidelines for Computer and Network Facilities

The University strives to provide fair and distributed access to information technology (i.e., computer and network) facilities for a large number of users. The acceptable use guidelines that follow apply equally to all types of electronic information services, including electronic mail (e-mail) and electronic news groups, provided on WMU’s computer and network facilities. Everyone using University information technology resources is responsible for following guidelines that characterize acceptable use.

1. WMU supports the principles of academic freedom and free inquiry and expression in the online environment as well as in the classroom. This freedom must be balanced, however, with the responsibility not to infringe on other individuals’ rights.
2. Acceptable use of shared information technology facilities follows the same standards of common sense, courtesy, and restraint that govern the use of other public facilities. WMU regulations VIII K Sexual Harassment Policy and VIII Q Cultural Diversity Policy also apply to the online environment. Acceptable use requires users to be ethical and respectful of the rights of others and of the diversity of the University community, and to maintain a climate that does not interfere with the studies, work, or living environment of any members of the WMU community.
3. Acceptable use of information facilities respects individuals’ rights to privacy and to freedom from threats, intimidation, harassment, and unwarranted annoyance.
4. Acceptable use includes the right of individuals to access and save any legal files on the Internet. It is not acceptable to display and print potentially offensive material in public computer labs where others cannot avoid seeing these files. Such material should be viewed in a private location. Material that is potentially offensive to others should not be publicly displayed without an academic reason.
5. Acceptable use standards require everyone to take prudent and reasonable steps to prevent unauthorized access. Access authorization relies on user identification and password for each user. The user ID forms the basis for mechanisms that are designed to establish ownership and responsibility for computing resources and use. Acceptable use respects these identification and security mechanisms.
6. Acceptable use requires that all users refrain from any illegal and improper intrusions into the accounts of others and/or into any University information technology resources and systems.
7. Acceptable use requires that all users recognize and honor the intellectual property rights of others.
8. Acceptable use of information facilities respects University regulations, contracts with University suppliers, and all local, state, and federal laws. Software theft, also known as software piracy, is a topic of much concern. Acceptable use of software respects all associated license and/or purchase agreements; if you have not met the conditions of such an agreement for a given software package, do not copy the package for your use.
9. Acceptable use of all off-campus network connections (i.e., use of the Internet) respects the University’s network access contracts that impose strict requirements. In general, off-campus network use must be for education or research. The University’s access contracts prohibit commercial activities such as advertising. They also require all users to promote efficient use of the network to minimize and avoid, if possible, congestion of the network that interferes with the work of others.
10. Acceptable use of information technology resources requires that all users refrain from acts that waste resources and prevent others from having broad access to University computers and resources.

#### Enforcement

When instances of unacceptable use come to its attention, the University will investigate them and may take action to prevent their further occurrence. During an investigation, the University reserves the right to copy and examine any files or information residing on University systems allegedly related to improper use, including the contents of electronic mailboxes. Investigations that discover improper use may cause the University’s authorized investigators to

1. limit the access of those found using facilities or services improperly;
2. disclose information found during the investigation to other University authorities;
3. begin discipline actions as prescribed by University policies and procedures;
4. install automatic measures to limit improper use.