

# MARSHALL UNIVERSITY BOARD OF GOVERNORS

## Policy No. IT-1

### INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

#### 1 General Information:

**1.1. Scope:** This policy set standards of acceptable use of the information technology environment at Marshall University.

**1.2 Authority:** W. Va. Code §18B-1-6

**1.3 Passage Date:** March 8, 2006

**1.4 Effective Date:** Upon passage

**1.5 Controlling over:** Marshall University and Marshall Community and Technical College

#### 1.6 History:

1.6.1 Statutory References:

1.6.2 This policy replaces the original Computer Use and Abuse Policy and is authorized by the Information Technology Council effective April 8, 2005

#### 2 Policy:

##### 2.1 Introduction

Information technology is playing an increasingly important role in the life of each individual, and consequently to the Marshall University community. Access to these finite resources is a privilege and is provided with an expectation of responsible and acceptable use. In addition to the principles and guidelines provided in this policy, institutional policies along with certain federal, state and local regulations apply to the use of the information technology environment (ITE).

##### 2.2 General Principles and Guidelines

The basic premise of this policy is that responsible and acceptable use of the Marshall University ITE does not extend to whatever an individual is capable of doing. Instead, certain principles provide a guide to users regarding responsible and acceptable behaviors and users are responsible for knowing and understanding them. These principles and guidelines include, but are not limited to:

2.2.1 The Marshall University ITE was funded and developed for the sole purpose of promoting and supporting the mission of the University.

2.2.2 Authorized users of the Marshall University ITE, or University sponsored resources such as WVNET and RuralNet, are those individuals who have been granted a username and password. The username and password combination is your identity and license to access and use the components of the Marshall

University information technology environment for which you are specifically authorized.

- 2.2.3 Authorized users will abide by institutional policies along with applicable local, state and federal regulations.
- 2.2.4 The resources of the Marshall University ITE are finite and shared. Appropriate and responsible use of these resources must be consistent with the common good. The ITE may NOT be used for commercial or profit-making purposes.
- 2.2.5 The University reserves the right to limit access to the Marshall University ITE when investigating cases of suspected abuse or when violations have occurred.
- 2.2.6 The University does not monitor or generally restrict the content of material stored on or transferred through the components of the ITE. Use of the ITE is a privilege and not a public forum, therefore the University reserves the right to restrict or deny usage of the ITE when such usage does not promote or support the mission of the University.
- 2.2.7 Users must adhere to the ethical standards governing copyright, software licensing, and intellectual property.
- 2.2.8 Personal web pages may NOT contain the official Marshall University logo.

### **2.3 Enforcement**

Violation of these guidelines constitutes unacceptable use of information resources, and may violate other University policies and/or state and federal law. Suspected or known violations should be reported to the appropriate University computing unit. The appropriate University authorities and/or law enforcement agencies will process violations. Violations may result in revocation of computing resource privileges, academic dishonesty or Honor Council proceedings, faculty, staff or student disciplinary action, or legal action.

The maintenance, operation, and security of computing resources require responsible University personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to the West Virginia Access to Public Records Act, other applicable state and federal laws, and the needs of the University to meet its administrative, business, and legal obligations.

### **2.4 Commentary: Introduction and analogies**

The Information Technology Environment discussed above consists, not only, of the superficial wires, equipment and devices of the data, voice, video, and more conventional information networks on our campuses (and the world!) but also the more subtle milieu created by the integration of these technologies into our everyday life situations. In this respect the whole is much greater than the sum of the parts and thus the effect of inappropriate use of this resource can be much greater than might be imagined. This

should not be a cause for hesitation about its use but merely a call for thoughtful consideration of action.

In describing the responsibilities and acceptable behaviors related to the Information Technology Environment, certain analogies can be drawn. Social norms, behaviors, and responsibilities associated with the use of electronic communication, publication, media, and access authorization are no different than the conventional mediums with which we are all familiar, i.e.,

Email or electronic mail is just another form of mail or communications,

Posting to a news group is the same as posting a notice or comment on a bulletin board, newsletter, letter to the editor, call to a talk show, etc.,

Participating in a chat group is the same as participating in discussions anywhere a group might congregate face-to-face e.g. in a class, the student center, recreation room, lounge, church group, etc.,

Creating a WWW or World Wide Web presence is publishing (i.e., making public) your own magazine, memoirs, diary, biography, press release, newsletter etc. Consequently, you are not only, typically, the author but also, perhaps more importantly, you become the editor and publisher and are responsible for your publication from a legal standpoint. Even though Marshall University is not the publisher, editor, or author it is the provider of the resource and, as such, is associated with your publication. Therefore, Marshall University maintains the right to restrict or deny use of this resource when usage does not promote or support the mission of the University or the State of West Virginia.

User ID and password combinations are your identity and license to use and access limited portions of the IT environment. In this sense they are like your MU identification card or a drivers license. Impersonating another individual, or allowing another to impersonate yourself is not acceptable behavior.

The computing systems used for mail, WWW, and other technologically augmented services are similar to a residence hall room, or assigned work or office space. The space (and some of the content) belongs to Marshall University and the State of West Virginia but other personal items in the room belong to you. In this sense MU has an obligation to provide a reasonable amount of security to protect your personal property but cannot assume full responsibility for it nor guarantee full privacy (if you are concerned about the inadvertent disclosure of information you should protect these items in another way).

Similarly, as in your residence hall room or office space, in the course of normal maintenance of the IT environment, certain information may be seen by those attending to the maintenance. All employees of Information Technology are instructed that the disclosure of this information is a punishable offense (as is the willful intrusion without cause). Also, in a similar manner, you are allowed the use of certain space and accouterments and are expected to utilize them in a responsible manner by taking proper care, providing reasonable security, and respecting the property and privacy rights of others occupying similar spaces and their assigned, and private resources.

## **2.5 Common Forms of Violations**

Although most users strive for acceptable and responsible use of the ITE, inexperienced users may unwittingly engage in behaviors that violate the principles and guidelines of responsible and acceptable use. To that end, this section outlines some of the more common forms of violations that occur. These examples should not be interpreted as an exhaustive list of violations. Questions regarding the appropriateness of specific behaviors should be directed to Computing Services.

- 2.5.1 Furnishing false or misleading information or identification in order to access another user's account
- 2.5.2 Using another person's username/password or letting someone else use your username/password
- 2.5.3 Investigating, reading or attempting to access another user's files without permission
- 2.5.4 Attempts to access or manipulate certain components of the information technology environment without authorization
- 2.5.5 Alteration of software, data, or other files without authorization
- 2.5.6 Disruption or destruction of equipment or resources
- 2.5.7 Using subterfuge to avoid being charged for computer resources or deliberate, unauthorized use of another user's account to avoid being billed for services
- 2.5.8 Copying or attempting to copy data or software without authorization
- 2.5.9 Sending mail or a program which will replicate itself or do damage to another user's account
- 2.5.10 Interfering with legitimate work of another user
- 2.5.11 Sending abusive, harassing, or obscene messages
- 2.5.12 Viewing or listening to objectionable, obscene, pornographic, or harassing material in public areas
- 2.5.13 Excessive recreational use of resources
- 2.5.14 Sending chain letters or unauthorized mass mailings or transmitting a crippling number of files across a network
- 2.5.15 Sending hoax messages or forged messages, including messages sent under someone else's username
- 2.5.16 Any activity or action that violates the University's Student Code of Conduct or Policies, faculty/staff policies and regulations, or federal, state, or local laws.

## **2.6 Enforcement**

Computing Services is authorized to engage in investigations and apply certain penalties to enforce this policy. These penalties include, but are not limited to, temporary or permanent reduction or elimination of access privileges to any or all of the components of

the ITE. If, in the opinion of Computing Services, it is necessary to preserve the integrity of facilities, services, or data, Computing Services may suspend any access, whether or not the account owner is suspected of a violation. In such a case, Computing Services will attempt to notify the user of any such action after the potential threat to the facilities, services, or data is contained. If such an investigation is required it will be done only under the direct authorization of the Executive Director of Computing Services and all effort will be made not to disclose any content to anyone other than those with a need to know during the investigation or adjudication of the alleged offense

Consequences of the discovery and investigation process or normal maintenance might include the inspection of files contained in an individual's storage space or monitoring selected traffic on the networks. Again, all effort will be made not to disclose any content to anyone other than those with a need to know. However, where there are moral, ethical, or legal implications of the nondisclosure of such information Computing Services personnel are similarly instructed to contact the Executive Director of Computing Services, who, may authorize its disclosure to appropriate authorities if deemed warranted.

In most cases an individual accused of a violation of this policy will be notified and have an opportunity to respond before a final determination of a penalty is made. The Executive Director of Computing Services or their designee, in conjunction with other responsible parties (e.g., University Counsel, Student Judicial Affairs, Academic Affairs, or Personnel) will examine the available evidence and circumstances. If a penalty is levied, the decision may be appealed through the appropriate channels.