card or a driver's license. Impersonating another individual, or allowing another to impersonate you 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.

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.

1. Furnishing false or misleading information or identification in order to access another user's account
2. Using another person's username/password or letting someone else use your username/password
3. Investigating, reading or attempting to access another user's files without permission
4. Attempts to access or manipulate certain components of the information technology environment without authorization
5. Alteration of software, data, or other files without authorization
6. Disruption or destruction of equipment or resources
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
8. Copying or attempting to copy data or software without authorization
9. Sending mail or a program which will replicate itself or do damage to another user's account
10. Interfering with legitimate work of another user
11. Sending abusive, harassing, or obscene messages
12. Viewing or listening to objectionable, obscene, pornographic, or harassing material in public areas
13. Excessive recreational use of resources

14. Sending chain letters or unauthorized mass mailings or transmitting a crippling number of files across a network
15. Sending hoax messages or forged messages, including messages sent under someone else's username
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.

Enforcement

Computing Services is authorized to engage in investigations and apply certain sanctions to enforce this policy. These sanctions 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 sanction 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 sanction is levied, the decision may be appealed through the appropriate channels.

EDUCATION RECORDS: PRIVACY RIGHTS OF PARENTS AND STUDENTS

(See Student Affairs Section)

MARSHALL UNIVERSITY DEFINITION OF DIRECTORY INFORMATION

The Family Education Rights and Privacy Act (Buckley Amendment) states that an educational institution may release without written consent those records identified as public or directory information for student who are currently enrolled provided that the institution informs the students of the categories defined as directory information and students are given an opportunity to refuse disclosure of any or all of the defined categories. Marshall University's policy statement defines directory information as follows: name, address, email addresses,