## ACCESSIBILITY/USE

All of the College's computer systems require that each user have a unique identity, protected by password, to gain access to the system. The computer identity is used to represent a user in various system activities, to provide access to certain software and data based on the user's credibility and purpose for requiring such access, and to associate the user's own software and data with the user's identity. As such, this computer identity is an instrument of identification, and its misuse constitutes forgery or misrepresentation. Conduct which involves misuse of computer identity is subject to College disciplinary action. This conduct includes:

1. Failing to change a password.

2. Intentionally seeking information about, browsing, obtaining copies of, or modifing files, passwords or tapes belonging to other people, whether at Wayne State College or elsewhere, unless specifically authorized to do so by those individuals. (Note: If an individual has explicitly and intentionally established a public server or clearly designated a set of files as being for shared public use, others may assume authorization.)

3. Decrypting or translating encrypted material or obtaining system privileges to which they are not entitled. Attempts to do any of these will be considered serious transgressions.

4. Failing to report a gap in system or network security. Users must refrain from exploiting any such gaps in security.

5. Interfering with the supervisory or accounting functions of the systems or engaging in actions that are likely to have such effects.

6. Displaying images, sounds or messages which could create an atmosphere of discomfort or harassment for others. Users must also refrain from accessing or transmitting to others in any location images, sounds or messages which might reasonably be considered harassing.

7. Tying up computing resources for game playing or other trivial applications; sending frivolous or excessive mail or messages locally or over an affiliated network; printing excessive copies of documents, files, images or data. Users must refrain from using unwarranted or excessive amounts of storage; printing documents or files numerous times because of not having checked thoroughly for all errors and corrections; printing more than one copy of any document; or running grossly inefficient programs when more efficient ones are available. Users must be sensitive to special need for software and services available in only one location and cede place to those whose work requires the special items.

8. Preventing others from using shared resources by running unattended processes, or placing signs on devices or otherwise disabling devices to "reserve" them without authorization. Absence from a public computer or workstation should be no longer than warranted by a visit to the nearest restroom. A device unattended for more than ten minutes may be assumed to be available for use, and any process running on that device may be terminated. Users must not lock or otherwise disable a workstation or computer which is in a public facility. Users must be sensitive to the performance effects of remote login to shared workstations; when there is a conflict, priority for use of the device must go to the person seated at the keyboard rather than to someone logged on remotely.

9. Copying, cross-assembling, or reverse-compiling programs/data under contracts/licenses. Users are responsible for determining that programs or data are not restricted before copying them in any form, or before reverse assembling or reverse-compiling them in whole or in any part. If it is unclear whether users have permission to copy such software or not, assume that such may not be done.

10. Altering or attempting to alter the "From" line or other attribution of origin in electronic mail, messages, or postings will be considered transgressions of College rules.

11. Creating, altering, or deleting any electronic information contained in or posted to any campus computer or network under any name other than the user's own; such acts will be considered forgery if they would be considered so on a tangible document or instrument.

12. Plagiarizing electronic data; if the use of the data from such media would be considered plagiarism on a tangible document or instrument it is considered so on electronic media.

13. Creating, sending or forwarding electronic chain letters.

Users should be aware that there are Federal, State and sometimes local laws which govern certain aspects of computer and telecommunications use. Members of the College community are expected to respect these laws, as well as observe and respect College rules and regulations.