

Vincennes University
Policy on the Use of Computers and Data Communications

I. PURPOSE

A. The University provides computer access and capabilities through the Management Information Center. The University relies heavily upon these systems to meet operational, financial, educational and informational needs. It is essential that VU's computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is critical that these systems and machines be protected from misuses and unauthorized access.

B. This policy applies to all University computer systems and refers to all hardware, data, software and communications networks associated with these computers. In particular, this policy covers computers ranging from mainframe systems to single user personal computers, whether stand-alone or connected to the network.

C. In addition to this computer policy, users of these computer systems are subject to applicable state and federal laws. Computer abuse will be referred to the Chief Information Officer or the appropriate person affiliated with the area where the abuse has occurred.

D. Computing resources are valuable, and their abuse can have a far-reaching negative impact. Computer abuse affects everyone who uses computing facilities. The same morality and ethical behavior that applies in the non-computing environment applies in the computing environment.

II. APPROPRIATE USE

A. Computing resources may not be used for any purpose that is illegal, abusive, or that is damaging to the reputation of the university, is inconsistent with the mission of the University, or is likely to subject the university to liability.

B. While University computing resources are to be used to advance the University's mission of education and public services and support the conduct of University business, the University acknowledges that occasionally faculty, staff and students use University computing resources for non-commercial, personal use. Such occasional non-commercial uses are permitted by faculty, staff and students if they are not excessive; do not incur significant costs; do not interfere with the efficient operation of the University; its employees, or its computing resources; are not prohibited by the supervisor or faculty; and are not otherwise prohibited by this policy or any other University policy or directive. The University will not provide technical support for any use not directly related to University business.

III. COMMON FORMS OF COMPUTER ABUSE

Abuse of computers, computer systems, computer networks, programs, and data is prohibited. The following are considered to be abuse:

A. Privacy *versus* Open Records

Investigating or reading another user's files is considered the same as reading papers on someone's desk – a violation of their privacy. Reading protected files, by whatever mechanism, is considered the same as "breaking and entering." Violations include, but are not limited to:

- Attempting to access another user's computer files without permission;
- Supplying or attempting to supply false or misleading information or identification in order to access another user's account;
- Deliberate, unauthorized attempts to access or use University computers, computer facilities, networks, systems, programs or data;
- The unauthorized manipulation of University computer systems, programs or data;
- The unauthorized capturing of computer network data directly from network backbone or local area networking media.

The university has the responsibility to protect, to the extent possible, confidential information concerning university citizens, such as social security numbers and other information that could compromise their privacy. In carrying out this responsibility, the University maintains firewalls and other software programs to secure its systems and networks. This includes the ability to track the source of unauthorized attempts to access, manipulate or use University systems and networks. The University reserves the right to prosecute criminally and to sue civilly individuals who engage in such "hacking" against the University.

B. Harassment

Harassment of other users consists of sending of unwanted messages or files. Violations include, but are not limited to:

- Interfering with the legitimate work of another user;
- The sending of abusive or obscene messages via computers;
- The user of computer resources to engage in abuse of computer personnel or other users;
- The sending of non-University related material to "All Users" (spamming).

C. Theft

Theft includes the stealing of any property of the Institution. Violations include, but are not limited to:

- Deliberate, unauthorized use of another user's account;
- Attempting unauthorized access to computers, inside or outside the University using the University's computers or communications facilities;
- Removing any computer equipment (hardware, software, data, etc.) without written authorization;
- Copying, or attempting to copy, data or software without proper authorization.

D. Vandalism

Any user's account, as well as the operating system itself is a possible target for vandalism. Attempted or actual alteration of user system software, data or other files, as well as equipment or resources disruption or destruction, is considered vandalism. Violations include, but are not limited to:

- Sending either mail or a program which will replicate itself or do damage to another user's account;
- Tampering with or obstructing the operation of the University's computer systems (for example, attempting to "crash" the system);
- Inspecting, modifying, or distributing data or software without proper authorization or attempting to do so;
- Attempting to interfere with the performance of the system;
- Damaging computer hardware or software.

E. Unauthorized Business Usage

Unauthorized Business Usage includes any use of University resources for promoting or conducting business for personal use. Violations include, but are not limited to:

- Sending mass mailings
- Using computers accounts for work not authorized for that account.

F. Copyright Violation

All members of the University community should be aware that copyright laws apply to the electronic environment. Users must abide by all software licenses, University copyright and software policies and procedures, and applicable federal and state law.

G. Miscellaneous

Other uses commonly considered abusive, such as:

- Unauthorized and time consuming recreational game playing;
- Using computer accounts for work not authorized for that account;
- Sending chain letters or unauthorized mass mailings;
- Using the computer for any illegal purposes.

IV. COMPUTER USAGE GUIDELINES

A. Users are to have valid, authorized accounts and may only use those computer resources, which are specifically authorized. Users may only use their account in accordance with its authorized purpose. Users are responsible for safeguarding their own computer account. Users should not let another person use their account unless authorized by the system administrator for a specific purpose. Passwords should be changed often to ensure that private and secure files are kept secure.

B. Home pages created by University faculty and staff and representing courses or products of the University are subject to review by and approval of the appropriate College Office or a designee.

C. Users may not change, copy, delete, read or otherwise access other users' files without the permission of the owner of such files. Only system administrators and those acting under their direction may change, copy or delete applications or system software. Users may not bypass accounting or security mechanisms to circumvent data protection schemes. Users may not attempt to modify software except when intended to be user customizable.

D. Users may neither prevent others from accessing the system nor unreasonably slow down the system by deliberately running wasteful jobs, playing games, engaging in non-productive or idle chatting, or sending mass mailings or chain letters, or maintaining or operating servers, shared drives or resources through or on the University connection, not related to University business

E. Users shall assume that any software they did not create is copyrighted. They may neither distribute copyrighted proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets.

F. A user shall disclose to the appropriate authorities misuses of computing resources or potential loopholes in computer systems security and cooperate with the systems administration in the investigation of abuses. However, the investigating parties shall maintain full documentation of such an inquiry or investigation, indicating reasons or probable cause prompting such an inquiry.

V. FREEDOM OF EXPRESSION AND PRIVACY

A. Vincennes University acknowledges that privacy and freedom of expression are fundamental values for educational institutions. Creative, innovative, and risky thought as well as scholarship and educational accomplishment all depend on interacting in a communication context in which individuals feel free to express and transmit their opinions and ideas. Consequently, it is the intent of the University to promote and protect the right to privacy and freedom of expression within the electronic environment to the extent possible. However, such protections are neither a guarantee of privacy in all circumstances, nor a license for abuse or improper use of the University's computing resources and facilities. Indiana and federal law, administrative reviews, computer system administration, audits, and the nature of the electronic medium itself mitigate privacy.

B. The University provides security measures to protect the integrity and privacy of electronic information such as administrative data, individual data, personal files, and electronic mail. All FERPA (Family Educational Rights and Privacy Act) requirements are followed. While computing resources are system property and all rights are retained regarding them, these rights will be balanced with a reasonable and legitimate expectation that technical staff and administrators will not monitor traffic content or search files except in compliance with the policy and procedures described in Section VI.

C. The content of files shall be examined only when there is a reasonable suspicion of wrongdoing or computer misconduct as determined by the Chief Information Officer and appropriate university authorities and with notice as required by Section VI. Examination of files shall be limited to the matter under consideration. Disciplinary matters involving computer and network systems shall be handled in accordance with the procedures described in Section VI.

D. Censorship is not compatible with the goals of Vincennes University. Vincennes University shall not limit adult users' voluntary access to any information due to its content when it meets the standard of legality.

E. The University reserves the right to place reasonable restrictions on computer usage in order to insure maximum bandwidth availability for uses of the network which relate directly to supporting the University's primary mission of education and public service.

VI. PENALTIES AND PROCEDURES

A. The University is committed to providing due process to all University citizens in enforcement of this policy. In order to protect the rights of University citizens:

- 1) The Chief Information Officer shall notify all University citizens in writing of all user files by type or by name that are backed up or otherwise copied and stored on the University system and the purposes for such back ups or copies and shall provide all University citizens access to such notification on the University system.
- 2) The Chief Information Officer shall notify any individual University citizen, in writing and in advance, whenever the contents of any file or copy of a file (any file created, modified or edited by such individual or addressed to such individual) will be examined and the purpose of such examination. This notice is excused only in the event of a law enforcement officer, who is involved in an active criminal investigation, making a reasonable request to the University President not to give such notice, and the University President, acting in good faith, making a written finding that such an investigation is warranted and giving written direction to the Chief Information Officer not to give such notice.
- 3) The Chief Information Officer shall notify in writing any individual University citizen of any suspected abuse of the system by that citizen with a request to that citizen to end the abuse. This notice is excused only in the event of a law enforcement officer, who is involved in an active criminal investigation, making a reasonable request to the University President not to give such notice, and the University President, acting in good faith, making a written finding that such an investigation is warranted and giving written direction to the Chief Information Officer not to give such notice. If the citizen feels that their use of the system does not constitute abuse, the citizen may appeal in writing to the Provost who must grant a hearing to the citizen within 14 days of the appeal. The Provost must decide the appeal within 7 days of the hearing. Either side may appeal the Provost's decision to the President within 7 days of that decision.

B. Abuse or misuse of computing services may violate the above-specified terms, but it may also violate criminal statutes. Therefore, the University will take appropriate action in response to user abuse or misuse of computing services. Action may include, but not necessarily be limited to:

- Suspension or revocation of computing privileges. Access to all computing facilities and systems can, may or will be denied;
- Reimbursement to the University for resources consumed;
- Other legal action including action to recover damages;
- Referral to law enforcement authorities;
- Computer users (faculty, staff or students) will be referred to the appropriate office for disciplinary action.

C. It is the policy of the University to:

- Secure and keep private any information on the University system protected by state and Federal privacy laws.
- Provide to all University citizens and others ready and convenient access to any information on the University system that is made public under public record laws of the state or Federal government.
- Provide access to information in compliance to legal process of state and Federal courts of competent jurisdiction in all civil and criminal matters.

VII. RESPONSIBILITIES OF DEANS, DEPARTMENT HEADS, AND SUPERVISORS

A. Ensure that employees within a department receive opportunities to attend training courses that help them to comply with this policy and other applicable University policies.

B. Promptly inform appropriate computer system administrators when employees have been terminated so that the terminated employee's access to University computer resources may be disabled.

C. Promptly report ongoing or serious problems regarding computer use to the Chief Information Office and Director of the Management Information Center

VIII. DISTRIBUTION OF THIS POLICY

The University will insure that all users are aware of the policy by publishing it in appropriate media designed to reach all faculty, staff and students.

Approved by the Board of Trustees
February 27, 2002