DEPAUW UNIVERSITY
ELECTRONIC COMMUNICATIONS AND ACCEPTABLE USE POLICY
(01-07-2006)

I. INTRODUCTION

The University has adopted this Policy in part to: encourage employee and student productivity; maintain the integrity and security of its network and computing resources and electronic communication systems; preserve its academic and business interests; and protect confidential information. This Policy cannot and does not provide rules and requirements to address every possible situation that may arise. However, it does provide certain minimum standards and requirements with respect to electronic communication issues. The University reserves the right to change, revise or add to this Policy at any time with such notice as it deems appropriate.

Under its Intellectual Property policy, the University has granted to faculty members the intellectual property rights to materials they have authored (articles, books, software, manuscripts, syllabi and course materials) and the results of their research. Faculty members may be required to provide copies of course materials or research protocols if needed for personnel reviews, program reviews, or campus disciplinary proceedings, including the enforcement of this or other policies. All other aspects of the University's electronic communication facilities, including all equipment and data, messages, or other information transmitted, stored or maintained on or in such facilities, are and remain at all times the property of the University, unless otherwise expressly noted in a written confirmation signed by an authorized University official. However, such ownership shall not include any such information that is in violation of any University policy, including, but not limited to, this Policy.

DePauw University recognizes and honors the importance of academic freedom, and the provisions of the Policy will be enforced with respect to the teaching and research mission of the University.

II. POLICIES

A. Permissible Uses of Electronic Communication Facilities

1. Electronic communication facilities are intended to be used primarily for official University business, including employee and student academic pursuits, and employee administrative, personnel and/or business matters. However, reasonable use of University-owned or operated electronic communication facilities for non-commercial personal purposes is permitted if it does not entail a direct cost to the University, interfere with the completion of job responsibilities, impede network operations, or violate University policies, including, but not limited to this Policy. Should users make use of the electronic communication facilities to transmit personal messages, such messages shall not be treated with a higher standard of privacy than any other electronic communication. The University reserves the right to place additional restrictions on the personal use of its electronic communication facilities if necessary to conserve network resources for University purposes. Further, those using the University's electronic communication facilities must use such facilities in a responsible and lawful manner. Unlawful use of electronic communication facilities or use of such facilities which violates any University policy, including this policy, by any user, as determined solely by University officials, will be cause for the University to deny such user further access to such facilities and may be cause for other University disciplinary action, up to and including termination from employment or expulsion.

2. Consistent with this Policy, users may use the electronic communication facilities to initiate or receive electronic communication. Users should only use their own files, those that have been designated as "public" files, or those that have been made available to them with the knowledge and consent of the owner.

3. Users shall always keep all copyright and trademark notices intact on University or third-party materials that are received or disseminated in electronic communication. An authorized University representative shall be consulted if there is any question about the form of such notice.

4. Users of electronic communication facilities in all IS facilities (including any remote sites operated by IS) must: a) fully identify themselves (e.g., by showing a University ID card or other appropriate identification) to any IS staff member or student employee who requests such ID; b) act in an appropriate manner towards other users and IS staff; and c) respect and follow all applicable rules and any notices (e.g., those concerning hours of operation) posted in IS facilities.

B. Prohibited Uses of University Electronic Communication Facilities

1. Commercial Purposes

Electronic communication facilities shall not be used for commercial purposes unrelated to the business of the University or for any commercial purpose that has not been expressly authorized by the University.

2. Other Prohibited Uses and Restrictions

a. Electronic communication facilities shall not be used to access or transmit electronic communication which promote or contain offensive, unlawful or inappropriate content, including, but not limited to content that is slanderous, defamatory, harassing, vulgar, threatening, intimidating, offensive, or that promotes hate or violence; or which is racially inflammatory or inappropriate; or which is pornographic, or sexually offensive; or which consists of offensive comments based on gender, or any other content that denigrates or demeans persons on the basis of race, age, gender, national origin, disability, religion, sexual orientation or any basis protected by law. This prohibition shall not apply to educational and professional work that requires such access or transmission.

b. Users should not attempt any unauthorized connection to a host using electronic communications facilities.

c. Electronic communication facilities should not be used to transmit, copy, or store confidential information, except as authorized by University officials. Further, all users must exercise a great deal of caution in transmitting and storing confidential information due to the ease with which electronic communication may be reproduced, stored and/or redistributed. Users should be particularly cautious in using distribution lists if confidential information is being transmitted.

d. Electronic communication facilities should not be used in any way that may infringe upon the rights of the holder of any copyright or trademark. Downloading, copying or installing software or other data that is subject to copyright, trademark or other legal protection without appropriate authorization or license is prohibited. Information Services (IS) staff will not knowingly provide support for software that a user possesses in violation of the applicable license agreement. IS staff may ask for proof of ownership before helping users with their software. IS staff will not knowingly allow infringing copies or otherwise unauthorized copies of software to be installed on electronic communications facilities and will remove any such suspect software loaded onto electronic communication facilities.

e. Electronic communication facilities shall not be used in any manner that: is contrary to the University's interests; attempts to obscure, withhold or falsify the identify of the sender; impairs the electronic communication facilities in any way; attempts to gain access to the electronic communication of third parties (unless expressly authorized by such third party or by the University); interferes with, interrupts or obstructs the ability of others to use such facilities; is not related to the performance of an employee's job responsibilities or a student's academic work; and/or is not otherwise authorized by the University.

f. Electronic communication facilities shall not be used in violation of University policies or local, state or federal laws, rules or regulations.

g. Users shall not abuse or vandalize any electronic communication facilities. Users are to immediately report any observed or suspected instances of abuse or vandalizing of electronic communication facilities to University officials.

h. Users should relinquish public computing facilities that they are using if they are doing non-essential work when the computers are in heavy demand. Electronic communication facilities should not be monopolized.

3. Security/Breach of Security

a. Although the University uses various methods in an effort to secure its electronic communication facilities, the University cannot guarantee such security. Electronic communication and electronic communication facilities shall not be used to breach the electronic security of others. A breach of security includes, but is not limited to: any unauthorized attempt to compromise any electronic communication facility, including the use of network privileges, accounts, access codes, identifiers or passwords, or equipment; knowing and unauthorized interception, access, disclosure, disruption, damage, destruction or unauthorized alteration/modification of any electronic information, or electronic communication facilities, including software or hardware; and any unauthorized and intentional disruption or interference with others' use of electronic communication facilities.

b. Users of electronic communication facilities are responsible for protecting their personal account information and/or password. Any user holding a personal account and its password is, at all times, responsible for its use and all activity originating from that account or using that password. Any attempt to determine the passwords or personal account information of others is strictly prohibited.

C. Privacy

Although University email messages are encrypted by University systems as part of the regular transmission process, the University cannot guarantee the privacy of electronic communications, and users should not expect their use of electronic communication facilities will be private. Users who further encrypt an electronic communication must furnish the encryption key or software to the University upon request so that the University may fulfill its obligations under the provisions of this policy.

III. MONITORING AND DISCLOSURE

A. In General

The University reserves the right to monitor or disclose the content of any electronic communication sent, received or stored using electronic communication facilities. Monitoring, investigation, and examination of electronic content will only be conducted in connection with a specific event, such as the delivery of a warrant for search and seizure or other permissible events as listed in the Policy. Employees are not permitted to engage in the monitoring, investigation, or examination of electronic communication content without prior specific authorization of the Chief Information Officer as specifically permitted under the Policy. Employees do regularly monitor the performance of the University's computing resources, and the University reserves the right to install or update files on any University-owned computer to assure the performance or security of the campus computing environment. Use of the electronic communication facilities shall be deemed to constitute consent to allow the University to exercise its rights outlined in this Policy and agreement to abide by this Policy.

B. Monitoring and Disclosure

As the owner or operator of electronic communication facilities and a private institution of higher education, the University will monitor or disclose the content of the electronic communication of users only under the following circumstances:

1. A party to the communication consents; or

2. The communication is readily accessible to the public (examples include, but are not limited to, web pages, e-mails sent to a public mailing list, or a newsgroup post); or

3. The University has an administrative need to access an e-mail, voice mail or other electronic communication or electronic communication facilities (examples include routine maintenance, backup of data, monitoring of usage patterns, troubleshooting or investigation of an excessive use of network resources that adversely affects performance or protection of the University's rights or property); or

4. The University is furnished with reasonable information causing it to conduct a review or investigation of any electronic communication or the use of electronic communication facilities (examples include reports or evidence of hacking, identity theft, harassment, commercial card fraud). The University has sole discretion to conduct such a review or investigation under this Policy; or

5. The monitoring or disclosure occurs as a result of the University's obligations under local, state and/or federal laws, rules or regulations.

IV. RETENTION AND ARCHIVAL STORAGE OF ELECTRONIC COMMUNICATIONS

A. Policies

Records created or stored in digital format, including electronic communication, may be subject to state or federal laws or University record-keeping policies.

B. Employee Responsibilities

Employees are responsible for copying electronic communication for storage in departmental or office files as required by law or University policy.

1. The University does not maintain centralized or distributed archives of electronic communication sent or received over its electronic communication facilities. Backups made for maintenance or troubleshooting purposes are erased at regular intervals.

2. Staff should periodically store such copies in departmental or office files for subsequent review followed by either archival storage or destruction in accordance with general University record-keeping policies.

V. ACCEPTANCE OF ELECTRONIC SIGNATURES

A. In General

[User] understands and agrees that by clicking the "I ACKNOWLEDGE" button the [User] is electronically signing the Request for Release of Educational Records or is authorizing specific University action and that the electronic signature is [User]' s valid and binding signature for purposes of the

Educational Records and authorization. [User] understands that: (1) All representations, information and electronic signature(s) [User] provides have the same force and effect they would have if made in non-electronic form; (2) DePauw University can and will rely on the Request for Release of Educational Records; and, (3) [User] intends to be bound to and electronically sign the Request for Release of Educational Records or other authorization by clicking the "I ACKNOWLEDGE" button.

[User] further agrees that Indiana's version of the Uniform Electronic Transactions Act (the "Act") applies to the Request for Release of Educational Records, that the Request for Release of Educational Records is a transaction for purposes of the Act, and the [User] consents to the exclusive jurisdiction of Indiana courts in resolving any conflicts arising out of the Request for Release of Educational Records.

VI. VIOLATIONS

Violations of this Policy by any user will be cause for the University to deny such users further access to the electronic communication facilities and may result in disciplinary action, up to and including termination from employment or expulsion. In certain circumstances, violators may be prosecuted. Violations of this Policy or the alleged misuse of University electronic communication facilities should be reported to the Public Safety Office, the Human Resources Office, or the Chief Information Officer. Reports and violations will be investigated and adjudicated according to the applicable University policies and procedures. The University reserves the right to delete any electronic communication from its electronic communication facilities that violates any provision of this Policy or any other University policy.

VII. RELATIONSHIP TO OTHER UNIVERSITY POLICIES

This Policy is a supplement to other University policies including, but not limited to, policies governing the appropriate or acceptable use of University property and/or electronic communication facilities.

VIII. DEFINITIONS

1. "Confidential information" means any information, data, documents or tangible things which contain proprietary or private information including, but not limited to information not generally known to persons outside of the University concerning students, academic or business matters, donors, alumni, financial or scholarship matters, grant matters, personnel matters, trade secrets, and/or development or business plans.

2. "Direct cost" means a cost, fee or charge assessed for a product or service provided for some purpose other than a valid University purpose (for example, unauthorized long-distance telephone charges and printing costs).

3. "Electronic communication" includes, but is not limited to, electronic mail ("e-mail"), newsgroup posts, internal or external bulletin board posts, Internet or World Wide Web pages ("web pages"), data and file transfers, voice mail, telephone and pager messages, facsimile transmissions, any other electronic communication sent, published, or received by an employee, student or guest using electronic communication facilities, and any other information transmitted, stored or maintained in or on such electronic communication facilities.

4. "Electronic communication facilities" includes, but is not limited to, all University-owned or operated: equipment, data, telephones, computers, computer networks, servers, workstations, personal computers, removable media, electronic voice mail systems, e-mail systems, pagers, facsimile machines, scanners, electronic external or internal bulletin boards, wire services, on-line services, the Internet or World Wide Web, or any other communication system or electronic technical resource provided, owned or operated by the University.

5. "Monitor" and “monitoring” mean to intercept, access, or inspect an electronic communication with the purpose of viewing the data contained therein. "Monitor" does not include automatic scanning of an electronic communication by network security and performance software such as a firewall, anti-virus, or packet shaper program.

6. "Employees" means any and all full- and part-time, temporary and regular University employees including, but not limited to faculty members, administrators, instructors, staff members, classified personnel and student employees who have been authorized to use the electronic communication facilities.

7. "Students" means any and all students who have paid a deposit or are currently enrolled in the University, as well as former students who have been authorized to use the electronic communication facilities.

8. “Guests” means any and all persons not directly connected to the University, but who have been authorized to use the electronic communication facilities.

9. "University authorization", "University authorized", or authorization from the "University", a "University official", or "University officials" means any written or oral express permission granted by one of the following University representatives: the President, the Vice President of Academic Affairs, or the Chief Information Officer.

10. "User" means any and all employees, students and guests.

11. "IS" means University Information Services.