Use of Technology at Notre Dame College

The Notre Dame College Acceptable Use Policy (AUP) promotes the efficient, ethical, and lawful use of Notre Dame College's information technology resources. The College's computing systems, networks, and associated facilities are intended to support the College's mission and to enhance the educational environment. Any use of these resources deemed inconsistent with the mission and purpose of the College will be considered a violation of this policy.

Scope

This policy applies to anyone who uses the College's information technology (IT) resources. The resources covered by this policy include, but are not limited to: computer hardware and software, data networks, and electronically stored data. Use of these resources includes access from off campus and on campus, as well as access from privately owned PCs and laptops.

Rights and Responsibilities

Employees and students may use College-owned IT resources for instructional, research, or administrative purposes. Access to and use of the Notre Dame College IT resources and the Internet shall comply with federal laws, the laws of the state of Ohio, and the rules and regulations of the College. Misuse of these resources may result in criminal charges. By using Notre Dame College's IT resources, all users agree to the rules, regulations, and guidelines contained in this Acceptable Use Policy. Computers and networks provide access to resources on- and off-campus, as well as the ability to communicate with other users worldwide. Such open access is a revocable privilege and requires that individual users act responsibly. This AUP is intended to supplement College Policy and does not release users from compliance with any existing policies that address ethical issues such as harassment, academic dishonesty, and plagiarism. The College's computers and networks are shared resources, for use by all employees and students. Any activity that inhibits or interferes with the use of these resources by others is not permitted. The College will ensure reasonable use by monitoring access logs, traffic data, and network utilization. Users are responsible for all activities to and from their network accounts. Users must take every precaution to protect logins and passwords. Under no circumstances should a user allow someone else to share a network or e-mail account. Users should not assume or expect any right of privacy with respect to the College's IT resources. Although the College does not seek to monitor the communication of its employees or students, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, that have been corrupted or damaged, or that may threaten the integrity of the College's computer systems. **In addition, files, e-mail, access logs, and any other electronic records may be subject to search under court order.**

Prohibited Use of Information Technology Resources

It is a violation of this policy to:

1) Intentionally and without authorization, access, modify damage, destroy, copy, disclose, or take possession of all or part of any computer, computer system, network, software, data file, program, or database. This includes:

a. Gaining access by willfully exceeding the limits of authorization

b. Attempting (even if unsuccessful) to gain unauthorized access through fraudulent means

c. Gaining access by using another person's name, password, access codes, or personal identification

d. Attempting (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes

2) Giving or publishing a password, identifying code, personal identification number or other confidential information about a computer, computer system, network or e-mail account, or database

3) Installing any software on computer systems in the computer labs, unless authorized by a member of the lab staff or a faculty member

4) Transferring copyrighted materials to or from any system, or via the College network, without the express consent of the owner of the copyrighted material. (See section entitled "File Sharing and Copyright Infringement.")

5) Providing outside access to College-developed or commercially-obtained network resources

6) Using any College IT resource for commercial, political, or illegal purposes, or for harassment of any kind

7) Displaying obscene, lewd, or otherwise offensive images or text

8) Intentionally or negligently using computing resources in such a manner as to cause congestion and performance degradation of the network

Provisions for Private Computers Connected to the College Network

The following apply to anyone connecting a private computer to the College network via the College Housing network, wireless LAN connection, dial-up network connection, or a regular network connection in an office.

1) The owner of the computer is responsible for the behavior of all users on the computer, and all network traffic to and from the computer, whether or not the owner knowingly generates the traffic.

2) A private computer connected to the network may not be used to provide network access for anyone who is not authorized to use the College systems. The private computer may not be used as a router or bridge between the College network and external networks, such as those of an Internet Service Provider.

3) Should the IT staff have any reason to believe that a private computer connected to the College network is using the resources inappropriately, network traffic to and from that computer will be monitored. If justified, the system will be disconnected from the network, and action taken with the appropriate authorities.

4) Any residential student, with an authorized network account, may use the in-room connection for scholarly purposes, for official College business, and for personal use, so long as the usage:

a. Does not violate any law or this policy

b. Does not involve extraordinarily high utilization of College resources or substantially interfere with the performance of the College network

c. Does not result in commercial gain or profit.

5) Users are responsible for the security and integrity of their systems. In cases where a computer is "hacked into," it is recommended that the system be either shut down or be removed from the campus network as soon as possible to localize any potential damage and to stop the attack from spreading. If you suspect electronic intrusion or hacking of your system and would like assistance, contact IT (x5227) immediately.

6) The following types of servers should never be connected to the College network: DNS, DHCP, and WINS, or any other server that manages network addresses.

Electronic Mail

The College e-mail system is not a private secure communications medium. As such, e-mail users cannot expect privacy. By using the College e-mail system, each user acknowledges:

1) The use of electronic mail is a privilege not a right. E-mail is for College communication, research, or campus business. Transmitting certain types of communications is expressly forbidden. This includes messages containing chain letters, pyramids, urban legends, and alarming hoaxes; vulgar, obscene or sexually explicit language; threatening or offensive content; derogatory, defamatory, sexual, or other harassment; and discriminatory communication of any kind. As with other information technology resources, the use of e-mail for commercial or political purposes is strictly prohibited.

2) Under the Electronic Communications Privacy Act, tampering with e-mail, interfering with the delivery of e-mail, and using e- mail for criminal purposes may be felony offenses, requiring the disclosure of messages to law enforcement or other third parties without notification.

3) E-mail messages should be transmitted only to those individuals who have a need to receive them. Distribution lists should be constructed and used carefully. E-mail distribution lists should be kept current and updated regularly. Inappropriate mass mailing is forbidden. This includes multiple mailings to newsgroups, mailing lists, or individuals (e.g. "spamming," "flooding," or "bombing").

4) All users of the College e- mail system waive any right to privacy in e-mail messages and consent to the access and disclosure of e-mail messages by authorized College personnel. Accordingly, the College reserves the right to access and disclose the contents of e-mail messages on a need-to-know basis. Users should recognize that under some circumstances, as a result of investigations, subpoenas, or lawsuits, the College might be required by law to disclose the contents of e- mail communications.

Printing

College printers are to be used for Notre Dame College class work or business. Limited personal use of College printers is allowed however printing large quantities such as materials for courses taught at other institutions is prohibited unless approved in advance by College administration.

Laptops

It is the faculty/staff member's responsibility to take appropriate precautions to prevent damage to or loss/theft of your laptop computer. The faculty/staff member or department may be responsible for certain costs to repair or replace the computer if the damage or loss is due to negligence or intentional misconduct. If the laptop is lost or stolen it must be reported to Information Technology immediately. For theft or loss off campus, it should also be reported to local police as well. The police report should include the serial number for the lost computer. A copy of the police report must be sent to IT within 48 hours.

File Sharing and Copyright Infringement

Federal copyright law applies to all forms of information, including electronic communications. Members of the College community should be aware that copyright infringement includes the unauthorized copying, displaying, and/or distributing of copyrighted material. All such works, including those available electronically, should be considered protected by copyright law unless specifically stated otherwise. Notre Dame College complies with all provisions of the Digital Millennium Copyright Act (DMCA). Any use of the Notre Dame College network, e-mail system, or Web site to transfer copyrighted material including, but not limited to, software, text, images, audio, and video is strictly prohibited. Therefore, the use of popular file sharing programs such as KaZaA, Morpheus, iMesh, Limewire etc. is, in most cases, a violation of College policy and federal law.

Reporting Violations of IT Acceptable Use Regulations

Violations of this Acceptable Use Policy should be reported immediately to the Chief Technology Officer, extension 5227. The College will make every effort to maintain confidentiality to the extent possible consistent with other obligations.

Disciplinary Action

Violations of these regulations will result in the appropriate disciplinary action, which may include loss of computing privileges, suspension, termination, or expulsion from the College, and legal action.