 <p>Ringling College of Art + Design</p> <p>STAFF HANDBOOK</p>	Index:	706
	Page:	1 of 4
	Subject:	Responsible Use of Electronic Communications
	Revised:	August 1, 1999

Responsible Use of Electronic Communications

Policy Statement

Ringling College of Art and Design provides an environment for the campus community to utilize appropriate computer and electronic information technologies in meeting the educational mission of the College. The College expects all members of its community to use electronic communications in a responsible manner. It is each individual's responsibility to become familiar with his/her rights and responsibilities as outlined in this and other appropriate College documents. There are also federal, state and local laws governing some aspects of information use and distribution. While guidelines may be provided in the context of the classroom, each individual is responsible to remain knowledgeable about current laws and policies.

Ringling College seeks to enforce its policies regarding non-harassment and the safety of individuals; to protect the College against damage or legal consequences; to prevent the electronic posting or distributing of copyrighted material in violation of license restrictions or other contractual agreements; to safeguard the integrity of computers, networks, and data, either at Ringling College of Art and Design or elsewhere; and to ensure that use of electronic communications complies with the student handbook, the faculty handbook and the staff handbook.

Ringling College of Art and Design may restrict the use of its computers and network systems for electronic communications in response to complaints presenting evidence of violations of Ringling College policies or codes, or local, state or federal laws. Specifically, the College reserves the right to limit access to its networks through Ringling College-owned or other computers, and to remove or limit access to material posted on Ringling College-owned computers. Ignorance of the law or of campus policies does not exonerate one from the consequences of inappropriate or illegal behavior.


What follows is a list of some of the potential behaviors associated with computer use that are considered violations of the Student Code of Conduct and Prohibitions for All Campus Members. This list is not intended to be exhaustive; it is simply to provide examples of some of the behaviors that are considered unacceptable. Any behaviors, including those not explicitly listed here, in violation of the Student Code of Conduct will be adjudicated accordingly.

Examples of Violations

A. Violations targeted at a specific individual(s)



- ◆ Sending harassing, threatening, communication by electronic mail or other electronic communications.
 - ◆ Sending harassing communication that is sexual in nature by electronic mail or other electronic communications.
 - ◆ Sending harassing communication or posting hate speech that is motivated by racial, ethnic, religious, gender or sexual orientations prejudice by electronic mail or other electronic communications.
 - ◆ Posting or otherwise disseminating personal or sensitive information about an individual(s).
- B. Violations causing harm to the activities and/or the institution**
- ◆ Propagating electronic chain mail.
 - ◆ Interfering with freedom of expression of others by “jamming” or “bombing” electronic mailboxes.
 - ◆ Forging, fraudulently altering, or willfully falsifying electronic mail headers, electronic directory information, or other electronic information generated as, maintained as, or otherwise identified as College records in support of electronic communications.
 - ◆ Using electronic communications to forge an academic document.
 - ◆ Using electronic communications to hoard, damage, or otherwise interfere with academic resources accessible electronically.
 - ◆ Using electronic communications to steal another individual’s works, or otherwise misrepresent one’s own work.
 - ◆ Using electronic communications to collude on examinations, papers or any other academic work.
 - ◆ Using electronic communications to fabricate research data.
- C. Violations involving illegal, proprietary, or damaging material**
- ◆ Electronically distributing or posting copyrighted material in violation of license restrictions or other contractual agreements.
 - ◆ Launching a computer worm, computer virus or other rogue program.
 - ◆ Downloading or posting illegal, proprietary or damaging material to a College computer.
 - ◆ Transporting illegal, proprietary or damaging material across College networks.
- D. Violations targeted at classes of individuals**
- ◆ Posting hate speech regarding a group’s race, ethnicity, religion, gender, or sexual orientation.
 - ◆ Harassing or threatening classes of individuals.

 <p>Ringling College of Art + Design</p> <p>STAFF HANDBOOK</p>	Index:	706
	Page:	3 of 4
	Subject:	Responsible Use of Electronic Communications
	Revised:	August 1, 1999

Responsible Use of Information Technology Resources

Guidelines

This statement defines the guidelines governing access to and use of information technology resources at Ringling College of Art and Design. These guidelines have been implemented to clarify and simplify procedures regarding use of information technology resources and to safeguard the computing and data network equipment.

All members of the Ringling College community are expected to utilize information technology resources in a responsible and appropriate manner, respecting the rights of other users. Each user is responsible for becoming familiar with his/her rights and responsibilities and applicable laws and guidelines. By utilizing these services, an individual agrees to abide by the guidelines and procedures that govern its use. Failure to abide by these guidelines and other applicable codes or local, state, or federal laws may result in disciplinary actions including, but not limited to, loss or limitation of privileges in using information technology resources.


Examples of Violations

Misuse of computing and information resources and privileges includes, but is not limited to, the following:

- Re-broadcasting unsolicited E-mail or USENET news (spam or electronic junk mail);
- Generating or forwarding chain letters, or participating in any kind of multilevel or pyramid scheme;
- Storing or transmitting copyrighted materials or licensed materials such as MP3 audio files without the owner's permission;
- Introducing viruses or other disruptive/destructive programs;
- Using resources such as network bandwidth or disk storage excessively;
- Attempting to evade or bypass resource quotas such as disk usage quota (logon to www.rsad.edu/manage.html to check your resource quotas);
- Attempting to decrypt coded information such as passwords;
- Using any Internet Protocol (IP) address inside or outside the Ringling domain(s) without prior approval;
- Attempting to install or utilize a server, network analysis tool, or network management tool on the Ringling College network without authorization;
- Intercepting network traffic intended for nodes other than your own.

Security and Confidentiality of Information Storage and Transmission

Ringling College of Art and Design cannot guarantee the confidentiality or privacy of electronic mail messages and other documents stored on College computers. Ringling

 <p>Ringling College of Art + Design</p> <p>STAFF HANDBOOK</p>	Index:	706
	Page:	4 of 4
	Subject:	Responsible Use of Electronic Communications
	Revised:	August 1, 1999

College assumes users are aware that electronic files and transmissions are not necessarily secure. Furthermore, electronic mail in its present form is not secured and has the potential to be vulnerable to unauthorized access, modification, and forgery. Such services should be utilized with this in mind.

The World Wide Web users should be aware that it is possible for software on a Web site to explore and retrieve information from the user's computer without the user being aware of the invasion. Anyone who "downloads" software, certain applications, or certain file types, or receives E-mail attachments should be aware of the possibility that such material could incorporate viruses, worms, or other destructive materials.

Guidelines Relating to Confidentiality

- Ringling College reserves the right to conduct routine maintenance, track problems, and maintain the integrity of its systems. As is the case with all data kept on Ringling College's computer systems, the content of electronic mail or user files may be revealed by such activities;
- Ringling College does not routinely monitor the contents of E-mail. However, such monitoring may be conducted when required to protect the integrity of the systems or to comply with legal obligations;
- Ringling College reserves the right to inspect the contents of electronic mail and all disk files in the course of an investigation into alleged impropriety or as necessary, to locate substantive information not readily available by other means, or to ensure compliance with institutional policy;
- Authorization to investigate the contents of user files or E-mails must be given by the Officers.

Responsibilities of System Administrators

System administrators shall perform their duties fairly, in cooperation with the user community, the appropriate higher-level administrators, and College policies. System administrators shall respect the privacy of users as far as possible and shall refer all disciplinary matters to appropriate authorities.