

Smoking Policy

Smoking poses a significant risk to the health of both the smoker and the non-smoker. Pursuant to NJSA 26:3D, effective March 1, 1986, the legislature finds that the right of the non-smoker to breathe clean air supersedes the right of the smoker to smoke. Effective March 28, 1994, the academic buildings of Stockton College became smoke-free. Smoking is prohibited in all academic buildings and vestibules (wings A through M). Smoking is also prohibited in the connectways between buildings and vestibules.

All Stockton employees, students and visitors are required to comply with this policy. Normal administrative disciplinary procedures or the appropriate negotiated agreement grievance procedure will prevail for employee violators. Student violators will be called before the Campus Hearing Board. In addition all violators are subject to prosecution under NJAC 2C:33-13 (Smoking in Public Places), which permits imposition of a fine of up to \$200.

P.L. 1981, C320 states that smoking shall be prohibited in any building used as a student dormitory that is owned and operated by a school or institution of higher education. All buildings in the Residential Hall Complex are designated as smoke-free. No smoking is permitted in these facilities at any time. In addition, no candles or incense are permitted in any buildings. Residents and guests are prohibited from smoking in all residence hall/apartment buildings.

Standards Concerning Acceptable Usage of Stockton's Computing Facilities

The purpose of this statement is to reaffirm the standards that apply in the matter concerning the acceptable use of The Richard Stockton College of New Jersey's computing and communication facilities, which include all computing, video, data and telecommunication hardware and software systems owned, leased or granted to the college.

These standards are defined and established to assure the integrity, reliability and availability of our computing facilities. The College is strongly committed to the goal of infusing advanced computer and communication technology into the fabric of the curriculum. Users are enthusiastically encouraged to explore and use the College's computing and communication facilities within the limits of these standards.

The standards set forth below apply to all users of Stockton College computing and communication facilities. Violations of any of these standards may result in revocation of facility usage privileges and/or appropriate disciplinary action under the College's Campus Code of Conduct or applicable federal and state laws and regulations, such as the New Jersey Computer Crimes Act, N.J.S.A. 2C:20-23, et seq.

The standards of acceptable computer and communication usage follow along with explanatory discussion of their intent and applicability.

Standard 1: Appropriate Use of Facilities:

Authorized use and access of the College's computing and communication facilities is intended and permitted solely to support the legitimate educational, administrative and mission-centered programs of the institution.

DISCUSSION:

Registered students may have access to these facilities for course-related instructional purposes. Members of the faculty and staff may have access to these facilities for institutionally recognized instructional or research purposes. Faculty and staff may also have access to administrative computing facilities, as needed, in accordance with their job responsibilities. Limited access to facilities may be granted to users such as Alumni Association members, government agencies, non-profit organizations or organizations that support the interests and needs of the College based upon any usage guidelines established by the College. Resident students in good standing may have access to telecommunication facilities for personal use on a fee basis and pursuant to the Housing Lease Agreement.

Authorization for use of and/or access to academic computing facilities is granted by the Assistant Vice President of Computer and Telecommunication Services. Authorization for the use of and/or access to administrative computing facilities is granted by the Assistant Vice President of Computer and Telecommunication Services and the Director or supervisor of the organizational unit that is the recognized custodian of the data for which access is requested.

Standard 2: Appropriate Use of Accounts:

Computer accounts and personal identification numbers (PIN) shall be used only by the individual authorized to use the account or PIN and only for the purposes for which the account or PIN was granted.

DISCUSSION:

Accounts or facilities are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions or for personal monetary gain that is inconsistent with College policy or federal and/or state statutes.

Users shall not disclose the password of an account or PIN or otherwise make the account or PIN available to others who have not been authorized to use the account or PIN. Users are responsible for all usage of their accounts and/or PINS and are expected to take appropriate safeguards to assure that their account passwords and/or PINS are not known to others.

Standard 3: Appropriate Use of Accessible Materials: Users shall observe discretion when viewing materials using the College's computing and communication facilities.

DISCUSSION:

Censorship is not compatible with the goals of The Richard Stockton College of New Jersey; however, some computers may be dedicated to specific research or teaching missions that limit their use. The College does not limit access to any information due to its content when it meets the standard of legality and is viewed in a proper time, place and manner. Forms of expression that are not protected by the First Amendment and therefore may be subject to censorship by the College include: obscene material, child pornography or other material that violates state or federal statutes.

Standard 4: Reliability and Integrity of Facilities:

Computer and communication facility users shall not knowingly develop, use or transmit through the College's facilities programs that harass other individual computer users or that interfere with, infiltrate or damage facilities.

DISCUSSION:

Computer and communication users shall use great care that they do not use programs or utilities or engage in actions which harass other individual computer users or that interfere with, infiltrate or damage facilities.

Any defects discovered in system security shall be reported immediately to the Assistant Vice President of Computer and Telecommunication Services.

Use of the electronic communication facilities (such as mail, phone, Internet or systems with similar functions) to send fraudulent, harassing, obscene, indecent, profane, intimidating or unlawful messages is prohibited. Additionally, users are prohibited from using electronic communication facilities to access or attempt to access remote computing facilities without authorization from the remote site.

Standard 5: Rules and Regulations: Users shall respect the rules and regulations governing the use of facilities and equipment.

DISCUSSION:

Use and access of computing and communication facilities, including computing laboratories, computer networks, telephony equipment and remote facilities accessed through local or wide area networks must be in accordance with the rules and regulations that govern the use of facilities.

All users are responsible for knowing and adhering to usage rules and shall cooperate in the implementation of these rules.

Standard 6: Proprietary Rights: Users shall respect the proprietary rights of software and documentation.

DISCUSSION:

Computer software, documents or files protected by copyright are not to be copied from or into computing facilities, except as permitted by license or law. Additionally, the number of copies and the distribution of copies must adhere to copyright restrictions and/or provisions. Further, typewritten or machine-readable documents protected by copyright are not to be reproduced or copied, unless permitted by the copyright owner.

Standard 7: Privacy: Users shall respect the privacy of other users.

DISCUSSION:

Computer users shall not attempt or knowingly seek, provide, view, use, delete or modify information in or obtain copies of files or programs belonging to other computer or telephony users without the permission of those users. Searching through non-public directories, libraries or any other storage media to find unauthorized information is likewise prohibited. Further, computer users must not use the facilities to plagiarize or claim the intellectual or literary property of others.

Users granted access to administrative data in which individuals are identifiable must respect the confidentiality of these data as well as any federal/state statutory requirements. Disclosure of data pertaining to students, for example, should be in accordance with the Family Educational Rights and Privacy Act.

On most facilities, security systems are in place to prevent unwanted or unauthorized access. Any defects or weakness discovered in

security systems should be reported the Assistant Vice President of Computer and Telecommunication Services or appropriate authority in cases not involving facilities under the auspices of the Office of Computer and Telecommunication Services. Under no circumstances shall computer or telephony users, other than authorized system administrators, access or attempt to access system security programs or files.

Users of e-mail should know that electronic mail is recognized as the equivalent of a formal memorandum. The College's e-mail systems are used to store and forward official college documents and support the academic and administrative operations of the college. E-mail system files and messages are backed up to tape regularly as a precaution against accidental loss or hardware failure. Users are permitted to use their electronic mail account to receive limited unofficial or personal correspondence, provided such use does not adversely impact upon essential academic and administrative usage. E-mail systems in general are not highly secure. Users are therefore advised not to consider e-mail correspondence private. The contents of the College's e-mail systems may be subject to disclosure under a subpoena in connection with a criminal investigation, or other authorized procedures including requests made pursuant to the Open Public Records Act (OPRA).

System administrators, operators or other authorized staff are allowed full access to files and programs during maintenance, routine backup operations, or in acting to safeguard the integrity and reliability of computing and communication facilities. Staff who are authorized such access shall respect the confidentiality of data stored. In the event that unauthorized computer or telephony system use is suspected, the staff member who detects or is informed of the suspected violation must notify the Assistant Vice President of Computer and Telecommunication Services or appropriate authority (See Standard 8).

Standard 8: System Safeguards:

Computing and communication facilities will be safeguarded to maintain the overall integrity and ensure reliability to all users.

DISCUSSION:

Where, in the judgment of the Assistant Vice President of Computer and Telecommunication Services or appropriate authority, an alleged violation of these standards or other regulations presents a risk to the integrity of the College's computing and communication facilities and/or the orderly conduct of the operation, computing and communication use privileges may be suspended on an interim basis and a hearing may be held pursuant to the procedure described in the Campus Code of Conduct.

Alleged violations also may be resolved informally pursuant to the procedure described in the Campus Code of Conduct under Informal Resolution or through the independent administrative action of the Assistant Vice President of Computer and Telecommunication Services or an appropriate authority provided both parties agree to resolve the case in this manner.

Stormwater Pollution Prevention

The College is mandated to comply with the New Jersey Stormwater Pollution Prevention Program, under N.J.A.C. 7:8, and New Jersey has enacted laws that require a public complex to adopt policies and procedures designed to protect against pollution resulting from stormwater runoff. (See N.J.S.A. 40:55D-95 et seq.) There are specific mechanisms designed within the laws for enforcement of the Program.

General guidelines and educational information about the plan follows:

A Guide to Healthy Habits for Cleaner Water

Pollution on streets, parking lots and lawns is washed by rain into storm drains, then directly to our drinking water supplies and the ocean and lakes. Fertilizer, oil, pesticides, detergents, pet waste, grass clippings: You name it and it ends up in our campus water such as Lake Fred or Moss Mill Stream. Storm water pollution is one of New Jersey's greatest threats to clean and plentiful water, and that's why we're all doing something about it. By sharing the responsibility and making small, easy changes in our daily lives, we can keep common pollutants out of stormwater. It all adds up to cleaner water, and it saves the high cost of cleaning up once it's dirty. As a student, it is important to know what you can do to protect our water:

- Stockton prohibits feeding the wildlife on campus, except at approved bird feeders. Do not feed wildlife such as ducks and geese on campus because their waste will be carried by stormwater into drains and eventually into Lake Fred. Excess nutrients can lead to nuisance algae blooms and harm fish.
- Don't litter: Place litter in trash receptacles.
- Recycle.
- Participate in community Water Watch cleanups.
- Dispose of cigarette butts in proper receptacles found on campus.
- Properly use and dispose of hazardous products. Hazardous products include some household or commercial cleaning products, lawn and garden care products, motor oil (motor oil may not be changed on campus), antifreeze, and paints. Do not pour any hazardous products down a storm drain because storm drains are usually connected to local waterbodies and the water is not