



STUDENT COMPUTER USE AND REGULATIONS POLICY

General Policy Statement

Kuyper College provides students with access to networks, computers, software and considers them a vital part of the educational experience. Students using these resources should do so responsibly and consistently with the College's values and purpose. Use of the network, computers, and software implies consent to the computer use and regulations policy and each student understands that any activity performed on a college resource (computer, email, web site access, or network) can and will be monitored. Enforcement of this policy will be handled at the College's discretion and may invoke discipline. Kuyper College reserves the right to define and enforce appropriate regulations at any point to ensure that the use of these resources is consistent with the College's values and purpose.

Additional Statements

Students are expected to minimize printing in the labs to help keep down the cost of providing the computer resources. Supplies such as laser toner and paper are provided for use in the laboratories on college-owned equipment. Printing should be limited to essential work and not personal use. Multiple copies of printouts (e.g., meeting notices, campaign posters, etc) should be made on photocopy machines rather than on the college provided computer printers. Supplies and equipment should not be removed from the laboratories for use on other equipment. Students with computers in their rooms are responsible for providing their own supplies for in- room use.

Students may use College owned computers and the College owned network for personal use as long as it is not their main focus. Students are not permitted to run any web resources such as web servers, chat rooms, or any similar services on the College owned network, College owned computers, or personal owned computers using the College's network.

Students violating the guidelines in this section may also be subject to criminal prosecution. The intent of these regulations is to ensure a productive and economical computing environment for all users, while abiding by laws governing copyrights and computer access. Questions and suggestions regarding these policies should be sent to the Information Technology Department.





STUDENT COMPUTER USE AND REGULATIONS POLICY

Student Guidelines

This section is not intended to impose restrictions on the resources provided by the college, but to help promote an environment that is both productive and consistent with the College's values and purpose.

Specifics

- All passwords are issued by the college and should be changed immediately. Passwords must be six (6) characters in length and should be complex enough so that it cannot be easily compromised. Students should ensure that their passwords are not shared to protect the students account and resources. If a password is compromised, then the student should contact the I.T. department to have it reset or reset it on their own.
- Because content is monitored, each student is responsible for the information stored in their account.
- Each student will be given storage on the network that will be limited to 300 megabytes. This will include their login profile.
- Each user is responsible for their own personal computers that might be used on the College's network. The same protection should be taken to ensure that student's personal resources are not compromised.
- All computer and network equipment is maintained by the Information Technology department and no person(s) should add equipment or software to Kuyper College's owned computers or the network without approval. Any computers, equipment, or software the user wishes to add to the network (wireless access points, hubs, switches, routers, dorm computers, etc) must be approved by the Information Technology department and might be subject to a fee.
- Email is provided for all students as a tool to help enhance learning, communications and productivity. The following are guidelines as to the proper use of email:
 - Student accounts are limited to twenty (20) megabytes. This includes all messages (sent, trash, received, and attachments).
 - Email (and profile) will be removed after one (1) month for graduating seniors or non-returning students. Exceptions can be made on a case by case basis by contacting the Information Technology department.
 - Information sent via email is not secure. Email can be intercepted and should be treated as public information.
 - Junk mail is unsolicited or unwanted e-mail of a non-academic nature. Sending junk mail and/or chain letters are prohibited. Junk mail and chain letters are a waste of system resources and the recipient's time.
 - If any user receives a harassing or threatening e-mail, that user should contact Kuyper College's Safety/Security and IT Departments immediately. Such e-mails violate Kuyper College's policy and may violate City, State, and Federal laws. Cyber-stalking is a crime.
 - E-mail, as with other forms of written messages/records, is subject to etiquette. Practical limits of freedom of expression do exist. There is a set of social codes that govern Internet communication. Please follow proper etiquette when sending email.
 - Unsolicited email is discouraged and prohibited to 25 recipients or more.





STUDENT COMPUTER USE AND REGULATIONS POLICY

Misuse of this policy will result in the following discipline specifics:

- Breaking or attempting to break computer security and/or using access to change or manipulate information will result in immediate dismissal.
- Violations that will result in **immediate loss of computer privileges** and may result in fines, suspension or dismissal are:
 - Transferring, or allowing/facilitating the transfer of, copyrighted materials to or from any system or via the College network without express consent of the owner is strictly forbidden (and is in violation of Federal and State Laws).
 - Introduction of harmful software such as worms, viruses, Trojan horses, or intentionally corrupting files.
 - Browsing, exploring, or making other unauthorized attempts to view data, files, or directories belonging to the College or to other users.
 - Possession of a program designed to gain unauthorized access, capture passwords, or perform other security breaches.
 - Accessing, viewing, displaying, printing, or distributing pornographic, inflammatory, discriminatory or obscene material, or establishing Web pages with links to such material.
 - Unauthorized use of another person's account.

