Purchase College Computer Ethics and Usage Policy

The Purchase College Information Technology infrastructure includes a private network of secure services for the exclusive use of our students, faculty, staff, and administrators. Other IT services include open access to College information for the general public and the world at large. To utilize private secure services for students, faculty and staff, you must authenticate with a Purchase College username and password.

Users of computer systems and networks at Purchase College must read, understand, comply with, and electronically sign the Purchase College Computing Ethics Policy when you activate your account. You are responsible for your actions. That responsibility exists regardless of what security mechanisms are in place. Unauthorized use of computing facilities will lead to suspension or loss of privilege, and may lead to more serious penalties. All rules and policies must be adhered to by all users of Campus Technology Services at Purchase College.

Appropriate use

All users are expected to use these services in a responsible fashion. Student use of all computing resources and services is subject to the Community Standard of Conduct. Faculty and staff use of computing resources and services is subject to the SUNY BOT policies and to campus supervisory oversight.

The College provides a variety of services that are public within the college community, and others that are public to the world. These services include (but are not limited to) our Portal, ePortfolios, Student Web Publishing Directories, sections of our website, and Moodle, among others. Materials posted to any College site or service must be respectful and appropriate - offensive materials or speech may be removed and/or referred to Student Affairs or the appropriate College supervisor.

Security for Your Account

Do not consider e-mail private or secure. Purchase College does not encrypt e-mail. Mail can be easily intercepted at any machine that it passes through. It can be altered and copies can be made and forwarded. Messages sent to nonexistent or incorrect addresses may be delivered to an unintended destination.

The systems administrator(s) at Purchase College have the right to monitor computer systems. The systems administrator(s) have the right to examine user files to diagnose system problems or investigate security breaches.

The Internet is not secure. If you are going to transmit sensitive data or files across the Internet you must take precautions to protect it on your own. Data and files can easily be intercepted, read, altered, misused or destroyed at any machine they pass through. In addition, machines attached to the Internet are vulnerable. Do not assume your data is safe on your computer if it is directly connected to the Internet. Do not store valuable or privileged information on these systems without applying security. If you can't afford to lose it, back it up. If it is information that should never see the light of day, don't store it on a networked computer.

Backup Your Important Data

Keep all valuable disks and tapes in a secure place. Secure backup copies of valuable files or data off site. When throwing out old disks or tapes, make sure no sensitive information can be found on them.

Intellectual Property and Piracy

Whenever you are shipping software from one place to another, you must consider intellectual property and license issues. The Internet is a global network, and the importing and exporting of software may fall under the jurisdiction of the United States Department of Commerce. Exporting anything may require a license. A general license covers anything that is not explicitly restricted, and is readily available in public forums in the United States. The exportation of networking code or encryption code is restricted. You may not allow access to a restricted machine to persons or entities outside of the United States. Please be aware when posting information to a bulletin board, that data will probably cross the border. If you have any questions on the legality of transmissions over the borders of the United States, please seek legal counsel.

Purchase College has joined Internet via an educational connection. Use of the Internet for commercial purposes is not allowed.

The following are considered unacceptable uses of computer systems, and are strictly prohibited

1. Deceiving a machine (i.e.: mimicking, imitating or attempting to use an ID other than your own)
2. Computer fraud (with and without intent to deceive)
3. Computer damage or destruction
4. Offenses against computer users including, but not limited to, harassment
5. Unauthorized use of any system
6. Modification or destruction of programs or data other than your own personal files
7. Use of computer to commit crime (embezzlement, harassment, blackmail etc.)
8. Tampering or alteration of computer, computer systems, programs or files
9. Unauthorized access or attempted unauthorized access to a computer or network
10. Causing denial of computer services (ex: run a virus that renders a network unusable)
11. Preventing others from using computer services
12. Causing deterioration of system performance (e.g. playing Doom over a network)
13. Computer trespass. This includes remote systems as well as secured areas of this system
14. Theft of computer related materials
15. Theft of computer services. For example, you may not use any pay service without paying
16. Computer invasion of privacy - unauthorized examination of files
17. Computer caused physical injury
18. Copying licensed software
19. Violation of any interstate laws applying to electronic transmissions
20. Violation of any import/export laws applying to electronic transmissions
21. Posting confidential information such as Social Security numbers or phone numbers
22. Cracking passwords
23. Even if a file is readable, do not assume you may read it unless explicitly granted authority to do so
24. Even if a file is able to be updated , do not modify it unless explicitly granted authority to do so
25. You may not share your account
26. You may not use any computer resource without prior permission
27. If a Purchase College systems administrator asks you to cease an activity on the computer, you must stop that activity immediately

Password Policy

Your password is the only means you have of keeping your account and files secure. The algorithm that encrypts passwords has not been broken. However, it is possible for your password to be stolen when using the Internet so you are encouraged to change it often. More than 80% of computer break-ins are because passwords can be easily derived by hackers.

The following requirements must be met when choosing a password:

1. Your password must be kept secret and changed often.
2. Your password must contain at least eight keystrokes, including the following in any order;
   choose at least 1 character from 3 of the four groups below:

- One or more uppercase letters (‘A’ through ‘Z’)
- One or more lowercase letters (‘a’ through ‘z’)
- One or more numerals (0 through 9).
- One or more non-alphanumeric keystrokes (Special Characters), including punctuation marks
  (including ` ~ ! @ # $ % ^ & * ( ) _ - [ ] { } ’ ” ~ / ? , . < > |).
  (it is best to include both numerals and punctuation marks.)

3. The space may be used in creating a password, or pass phrase. The space is not required and does not count as a Special Character, but does improve the complexity of a password. Most people find it easier to remember pass phrases than complex passwords. Combining words, spaces, digits and special characters can make a pass phrase that is both easy to remember and hard to guess.
   For example, **I’ll always have eyes 4 U** is a valid password.

4. Select a secure password that you are guaranteed to remember. An easy way to accomplish this is to join unrelated words, syllables, and/or letters that have special meaning only to you. Place non-alphabetic keystrokes between parts of words, syllables, or letters in your password. For example, “my Dog likes to eat Bananas and Strawberries” (note capitalized nouns) becomes “myD@wgl2eB&S”.
5. **Do not** use consecutive keys on the keyboard to form any significant part of a password (e.g. “ASD”, “qwerty”, “1234abcd”, “!@#”).
6. **Do not** use your login name to form any part of a password, nor use any common name, such as the name of a person or pet, nor any personal information (date, license number, etc...). Reversing these words is ineffective as well (e.g. the password “John.Smith” and “htimS.nhoJ” are equally ineffective, as is “1491/7/ceD”, or any form of a date).

Data Policy

Individuals who are authorized to access sensitive or institutional data are prohibited from divulging that data to any other individual, unless that individual is also authorized to use the data. Individuals are only permitted to access data as authorized.

Game Playing Policy

Game playing is allowed on College computers as long as:

1. It does not deteriorate system performance
2. The computer is not needed for school work, research or any other legitimate purpose

Hardware Policy

1. You may not move or take any hardware without explicit permission from the designated owner of that hardware.
2. You may not destroy or vandalize any hardware, cable or service provided by the campus.

Denial of Service

1. You may not disable the network by means of any computer program.
2. You may not disable the network by rendering any equipment unusable.

Security Policy

You are responsible for the security of your account. Please read the policy on passwords. The following are symptoms of unauthorized trespass of your account. If you become aware of the following, please contact CTS at x6465.

1. New or unexplained files found in your directory
2. Changes in file lengths or dates
3. Unexplained data modification or deletion
4. Unable to login to your account
5. Suspicious beeps, messages or pictures

VIOLATION OF THESE POLICIES WILL LEAD TO SUSPENSION OR LOSS OF PRIVILEGE, AND MAY LEAD TO MORE SERIOUS PENALTIES