NETWORK & RESPONSIBLE COMPUTING POLICY

Policy

1. University computer facilities and networks are available for exclusive use of registered students, faculty, and staff. To better serve the needs of users and emulate a corporate computing environment, the following policies are enforced by the Help Desk and IT staff. Users have a responsibility to be familiar with these policies and to abide by them. Users also have a responsibility to be familiar with and abide by related policies in the Student Code of Conduct.
2. All information services are intended for educational use and may not be used for commercial or other unauthorized purposes. Use of University computers, network facilities, application software, network disk space and the Internet is available for the purpose of coursework and support only. Communication via the Internet or networks is available for authorized users only.
3. Students are issued an account when they appear on the official class roster. All accounts are for the exclusive use of the person to which they are assigned and may not be “loaned” to other users. Other types of accounts may be applied for by completing an Account Request form at the Help Desk. A Help Desk assistant will check the user’s ID and sign the form indicating the ID was confirmed. All users will be given their own space on the network hard drive for storing course-related material and assignments. They may also receive access to specific software packages based on the judgment of the network administrator.
4. All passwords expire every 60 days. Student and alumni accounts will expire at the end of each semester. Chamberlain reserves the right to withdraw access to facilities or the network from any user, to withdraw all rights to any material stored in files, and to remove any harmful, unlawful, abusive, or objectionable material.
5. Chamberlain does not guarantee functioning of the system will be error-free or uninterrupted. The University cannot take any responsibility for files not protected through normal backup procedures.

Rules

1. Users may not attempt to alter workstation settings, including but not limited to, network configuration, Windows registry, virus checker settings or any other setting that might compromise security or performance of the University computer system. The IT department may implement workstation security software to monitor for and/or prevent users from making inappropriate changes to their workstations. Users are not permitted to store downloaded or commercial programs on the network or to install them on any University computer.
2. The privacy of other users must be respected.
3. Abusive or offensive language will not be used in any communications.
4. Students will not use the Internet or networks for illegal activities or to transmit unwanted or unsolicited advertising.
5. False statements made about any person and published on the Internet or networks constitute libel and may subject the student to civil charges.
6. The Internet or networks will not be used for transmitting chain or threatening letters.
7. Attacking or threatening messages are a direct violation of this policy. Users of the Internet or networks must abide by the same principles of fairness, decency and respect that would be expected in any other business environment.
8. Users will take ownership for all irresponsible activity/behavior exercised on the Internet or networks under their user login.
9. Material that may be considered offensive to others must not be displayed, stored, or printed on the University computer system.
10. Users of the Internet or networks must minimize the possibility of transmitting viruses or programs harmful to another user’s data or equipment by using an appropriate virus checker.
11. Sites with offensive material are not permitted. Internet chat rooms and online games are permitted as long as they do not cause disruption to normal academic related use or cause network congestion. Local or network game play is permitted under limited situations. Software is never to be installed on University computers and game play must never disrupt academic activities or cause network congestion. Determination of appropriate use and/or disruption of academic activities is at the sole discretion of University faculty or staff. Failure to comply with requests to cease any inappropriate or disruptive activity will result in revocation of any access, limited or otherwise, to online local or network games and internet chat rooms.
12. While most material on the network is considered to be in the public domain, copyright is breached if another user’s document is transmitted without user’s prior knowledge and permission. It is customary to acknowledge sources of any material quoted directly or paraphrased from elsewhere. See the policy on Academic Integrity for detailed information regarding the use and acknowledgment of other material.
13. It is illegal to use the Internet or networks to gain unauthorized access to other computers or databases not in the public domain.
14. Off-campus websites and email accounts created or accessed over the University computer network are subject to University policies and regulations.

Procedures

The IT department and Help Desk staff may periodically review files and communications to maintain system integrity and ensure users are using the system responsibly. Users should not expect that files stored on University servers will always be private. IT staff may also implement workstation management software, allowing them to monitor users’ activity for attempts to change settings or circumvent workstation security. All user activity including but not limited, to printouts, files, and email correspondence, may be monitored at any time for security purposes.

Sanctions

1. Any attempt by a user to breach workstation or network security or to tamper with a University computer, its software or the network will result in loss of computer access. Downloading material relating to hacking or malicious code creation will be considered an attempt at breaching network security. Any unauthorized software or hardware modifications found on the computer system will be removed.
2. Users who have their accounts disabled should contact the Help Desk to find out whom to contact to regain computer access. Minor violations may be resolved by the IT Department or Help Desk.

3. Major violations will be referred for further action under the Student Code of Conduct. Depending on the nature of the violation, other sections of the Student Code of Conduct may also apply.