Century Commons' Internet Use

Please Note: Even though you are unable to access the Internet, the sites below are always available. Open up Internet Explorer and type any of these in your address bar to access.

OC Blackboard server: http://blackboard.odessa.edu

OC website: http://www.odessa.edu

OC Student Email: http://www.odessa.edu/gmail

Windows update: update.microsoft.com

Anti-virus sites:
http://www.avast.com/eng/download-avast-home.html

http://free.grisoft.com/

Please Note: In order to provide a safe networking environment for the dorms, IT has implemented a server that will, verify student username, install a security agent on students computer, scan their computer for OS updates, anti-virus that is activated /w up to date signatures. The student username is the student's first name initial, last name initial, and student ID without leading zeros. (Example, Students name John Smith, Student ID 0088222, Students username will be js88222) IT will have to import student's username, before students can start the process of using the Internet. Also implemented is an intrusion protection system that will require the student to follow Odessa Colleges Internet usage policy shown below. In order to handle all internet related problems in a timely fashion, IT has implemented a Help Desk phone number just for the dorms, (335-6377) which will be checked by IT staff on a regular basis during normal college business hours. When students or staff call the help desk number, please provide a complete spelling of the students first and last name, student ID number, dorm room number, and correct phone number with area code. **Please do not call the Help Desk number until your computer has been updated with all Operating System updates and Anti-virus installed and updated.**

The registration process can be expedited by students having their computer OS updated, anti-virus activated and up to date, and making sure their computers comply with Odessa College's internet use policy before moving into their dorm room.

Peer-to-Peer File Sharing Programs Policy

The College does not allow the use of file sharing software for the following reasons.

1. This activity violates the College's policy which prohibits unauthorized servers. The Information Technology Department oversees or approves the operation of all servers on campus. Napster, LimeWire, Kazaa, Gnutella, FreeNet, BearShare, EDonkey, WinMX, BitTorrent, Morpheus, and other software of this type create a file sharing server whenever it is running on a network.
2. Several court cases have recently gone against the use of peer to peer and other types of file sharing software and the liability has been passed on to the businesses that allowed the software to be run on their networks, Odessa College does not allow any file sharing software to be run on its networks or computers. This includes PC's in the dorms as the networking and Internet connectivity in the dorms is provided by the College.
3. If any of these programs are installed on your computer, it will be quarantined and you will be unable to access the Internet.

Computer Information

Century Commons has a dedicated fiber connection with 3MB bandwidth for accessing the internet, including the Odessa College main site and Blackboard. To ensure that you have the fastest possible connection, there are a few things that are necessary to ensure the security of your computer and to enhance your connection speed.
As Operating System updates and Anti-Virus updates are released, your computer will have to be updated each time these are released. If your computer is in need of an update, you will be redirected to a web page that details the updates needed.

1. Keep your computer up to date with the latest patches from Microsoft.
2. Keep your computer virus free by making sure that your Anti-Virus software is up to date.
3. If you have anti-virus that came with your computer, the trial period may have expired. You may either purchase the anti-virus program or uninstall it and Install one the free anti-virus programs listed below.

Sites to update the Operating System and Anti-virus:

Microsoft Operating System Updates:
http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us

Free Antivirus Software:
To Install Avast Home Edition: http://www.avast.com/eng/download-avast-home.html
To Install AVG Free: http://free.grisoft.com/
To Update your anti-virus, open the anti-virus program and click update.

Odessa College
Use of Computer Resources Policy
Policy Date: Nov 2008

1.0 Overview

Odessa College acquires, develops, and utilizes computer resources as an important part of its physical and educational infrastructure. These computing resources are intended for college-related purposes, including direct and indirect support of the college's instruction and service missions; of college administrative functions; of student and campus activities; and of the free exchange of ideas among members of the college community and between the college community and the wider local, national, and world communities.

The rights of academic freedom and freedom of expression apply to the use of college computing resources. So, too, however, do the responsibilities and limitations associated with those rights. The use of college computing resources, like the use of any other college-provided resource, is subject to the normal requirements of legal and ethical behavior.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer resources at Odessa College. This policy is not intended to impose restrictions that are contrary to Odessa College's established culture of openness, trust and integrity. Rather, these rules are designed to promote efficient operations and to protect the college, its employees, and its students from illegal or damaging actions. Inappropriate use exposes Odessa College to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to all users of Odessa College computer resources, whether on campus or from remote locations. This policy also applies to all equipment that is owned or leased by Odessa College, including but not limited to phone systems, computer equipment, software, peripheral devices, operating systems, storage media, voice, video, data telecommunications systems, network accounts providing electronic mail, internet access, and any equipment connected to the College's network(s). As property of Odessa College, computer resources can be inventoried, examined or exchanged for other assets at any time the College deems necessary.

Additional policies may apply to specific computers, computer systems, or computer labs operated by specific departments. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

4.0 Policy

4.1 General Use

1. Any use of computer resources for commercial purposes, product advertisement, or political lobbying is prohibited.
2. Personal use of college computing resources must not consume a significant amount of those resources, must not interfere with the performance of the user's job or other college responsibilities, and must not result in personal financial gain. Further limits may be imposed upon personal use in accordance with normal supervisory procedures or specific departmental guidelines.

3. All use of computer resources must comply with applicable federal and state laws, other college policies, and all contracts and licenses. Examples include the laws of libel, privacy, copyright, trademark, child pornography, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the college's sexual harassment policy; and all applicable software licenses.
4. Users should be aware that the college cannot guarantee security of data. Pursuant to the Electronic and Communications Privacy Act of 1986, Odessa College's network administration desires to provide a reasonable level of privacy. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding and regularly changing passwords, and encrypting sensitive data.
5. Users should be aware that their uses of college computing resources are not completely private. While the college does not routinely monitor individual usage of its computing resources, Information Technology staff may monitor equipment, systems and network traffic on a periodic basis to ensure network integrity.

4.2 Security and Privacy

1. **Confidentiality:** Employees should take all necessary steps to prevent unauthorized access to or release of confidential information. The Family Educational Rights and Privacy Act (FERPA) will be adhered to in all matters regarding campus records. (Refer to the FERPA website for more information.)
2. **Passwords:** User level and administration level passwords for access to Odessa College servers and networks should be changed every semester. Passwords must contain a minimum of 6 characters, have not been used in the previous 3 passwords, do not contain your account or full name, and contain at least two of the following four character groups; English uppercase characters (A through Z), English lowercase characters (a through z), Numerals (0 through 9), and non-alphabetic characters (such as !, $, #, %). Authorized users are responsible for the security of their passwords and accounts. User names and passwords may not be shared with or used by persons other than those to whom they have been assigned.
3. **Colleague Access:** For access to the Colleague Administrative Database, the Data Processing & Colleague Services Department will assign each employee a unique login and password for use in accessing the Colleague Administrative Database. This password will give employees access to screens that can access the student, employee and budget data bases. What each employee can access will be determined by the appropriate supervisor/department head. The supervisor will also determine which employees will be able to update information on any of the Colleague databases.
4. **Software:** Only software that is properly licensed and approved by the IT Division will be purchased by the College. Software that is donated to the college must also be approved by the IT Division before it can be installed on any Odessa College computer.
5. **Postings to external newsgroups:** Postings by employees from an Odessa College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Odessa College, unless posting is in the course of business duties.
6. **External networks:** The College does not control and consequently cannot be responsible for the content of external networks. Any computer resource user, which traverses another network, must abide by the use policy of that network.
7. **Virus Scanning:** All computers used by the employee that are connected to the Odessa College Internet/Intranet/Extranet, shall use the IT division's approved virus-scanning software.
8. **Remote Access:** Odessa College remote access through the College VPN will require user's home PC to comply with all acceptable use policies including but not limited to maintaining current service packs, hot fix's, and anti-virus requirements. It is the user's responsibility to ensure that unauthorized users are not allowed access to the College internal network via the users home PC.
9. **College hosted websites:** Approval to setup web pages on the College's website must first be approved by the Division Dean. Upon approval, the Odessa College webmaster will provide space on the College's web server.
10. **Spyware and Virus Outbreaks:** In the event of a major virus or spyware outbreak, the IT Dept will quarantine a computer, which limits access to the network and internet, to protect the user and college

from information that might be sent off the campus. In the event a pc has been quarantined, a message will be displayed in the user's browser with instructions on what to do.

4.3. Unacceptable Use

Under no circumstances is an employee or student of Odessa College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Odessa College-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

Copyright Violations:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Odessa College.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted video, and other related items.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

Release of Confidential Information: Providing information about, or lists of, Odessa College employees and/or students to parties outside Odessa College.

Use of VPN: Use of VPN (Virtual Private Network) to access another network directly from the OC network is prohibited.

Unauthorized Hardware: Extending or adding to the campus network with any wireless, modem, or wired hardware is prohibited. (e.g., wireless access points, wireless routers, PDA's, wireless phones, contractor installed equipment, etc.) All network hardware must be installed and secured by the IT division or its authorized agents. Unauthorized servers are prohibited.

Unauthorized Computer Repairs: Repairing or modifying PC or network hardware without prior approval from the IT division is prohibited. IT personnel are trained and licensed to work on the PC and networking hardware purchased by the College. People other than the IT personnel working on College property may invalidate the product's warranty.

Unauthorized Use of Personal Laptop and PDA's on Campus: Employees that want to connect their personal laptops or PDA's to the campus network must complete the OC Personal Laptop form.

Prohibited Activities:

- Using an Odessa College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Any activities with the intention to create and/or distribute malicious programs into the network or servers are prohibited. (E.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- All file sharing programs such as Limewire, eDonkey, etc., are prohibited.
- Effecting security breaches or disruptions of network communication either on or outside of the campus network.
- Port scanning or security scanning is expressly prohibited unless prior notification to the IT division is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.

Prohibited Email and Communications Activities:

- Harassment: Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is prohibited.
- Impersonation: Unauthorized use, or forging, of email header information. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is prohibited.
- Pornography: Any use of computer resources for the production, duplication, distribution, receipt and/or transmission of any material, which might be considered pornographic under U.S. or Texas law is prohibited.
- Chain Letters: Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.

5.0 Enforcement

Users who violate this policy may be denied access to college computing resources and may be subject to other penalties and disciplinary action, both within and outside of the college. Violations will normally be handled through the college disciplinary procedures applicable to the relevant user. However, the college may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability. The college may also refer suspected violations of applicable law to appropriate law enforcement agencies.

The college may also specifically monitor the activity and accounts of individual users of college computing resources, including individual login sessions and communications, without notice, when there is reasonable cause to believe that the user has violated, or is violating, this policy or it is otherwise required or permitted by law. Any such individual monitoring must be authorized in advance by the President or the President's designees.

How to connect to the OC Dorm network for the first time

1. You will need a CAT 5 Ethernet Cable in order to access the network. These are available from most Office Supply or Electronics Stores.

2. There are 2 places to plug the cable into in your room, a red wall jack and a blue wall jack. Plug one end of the cable into the blue colored wall jack and plug the other end of the cable into your PC's ethernet jack. Modem connections will not work in your room.

3. After you have plugged the cable in open Internet Explorer and go to www.odessa.edu. If the page does not load try moving the cable to the red wall jack. If no page loads after trying both jacks call the Help Desk.

4. Use the Windows Update shortcut in your start menu to download all critical windows updates for your PC.

5. After the updates are downloaded and installed you will probably be asked to restart your computer. Depending on how long it has been since your computer was updated you may have to check for updates several times. After the computer restarts repeat the steps above until all available updates are installed and none are available.

6. You will now need to check and see if your Anti-Virus program is updated. Open the program you are using for Anti-Virus protection and find where you check for updates. If you had a free trial version that came with your PC you will have to purchase the program in order to get updates. If you don't want to purchase the program UNINSTALL the program through the control panel add remove programs feature and install one of the FREE Anti-Virus programs. If a free antivirus program is installed you will have to update it through the program interface as well.

7. Once ALL OS Updates and Anti-Virus updates are installed you will now need to install the security agent. Open Internet Explorer and try going to any website (i.e. www.google.com) you will be directed to a page that will begin the registration process. Click the start button to begin. After following the instructions you will be asked for your user name and password. Your username will be your first and last initials followed by your student ID number without the leading "0" (i.e. If your name is Allen Bates and your ID number is 0123456 your username will be AB123456) your password will be the last four digits of your social with OC in front (i.e. oc1234) If your username and password are not accepted please call the Help Desk.

8. After Authentication is successful you will see a page that has a link for the security agent. YOU MUST SAVE THIS FILE TO YOUR DESKTOP. Click save, do not click run when prompted. After the file is saved double click the program icon to install.

9. If you have updated your Anti-Virus and your Operating System with the most current available updates your computer will now access the internet. If you are missing updates you will be taken to a page that will tell you what needs to be updated on your computer. Do the needed updates and try getting out again.