Odessa College
Use of Computer Resources Policy
Policy Date: November 2010

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.
    a. All software to be purchased must be approved by the Dir of PC Services, Dir of Network Services, and the CIO of the IT Division
    b. Software licensing agreements and security measures vendors place on their application will be enforced and adhered to.
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. Users requesting VPN access must have their supervisor's approval. The request must be submitted by the supervisor before the users account can be setup.
9. **Remotely Hosted File Hosting/Synchronization Services (Cloud Storage):**
    a. Use of the service requires software approval (Form available in portal)
    b. College is not responsible for lost data when using these services.
    c. User must abide by any regulatory laws such as FERPA and copyright.
        i. User is restricted from placing any student related data in to the service. This includes items with grades or other student identifiable information.
    d. Users of these services are subject to random auditing of their data to verify compliance with FERPA and other laws.

10. **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.
11. **Spyware and Virus Outbreaks:** In the event of a major virus or spyware outbreak, the IT Dept will remove the computer from the network to protect the user and college from information that might be sent off the campus. Arrangements will be made for a loaner pc while pc is being repaired.
12. **Mobile Devices:** Use of mobile devices over the campus guest wireless network is granted. Users are responsible for the security of their mobile device and the data it contains.
13. **Wireless Network Access:** Odessa College provides wireless access to OC users. There are two wireless SSID's available to choose from.
    a. **OC-Guest:** This is provided for use by all students and all personal laptops and mobile devices. It has internet only access and is restricted from accessing the internal network.
    b. **OC-Faculty-WPA:** This is a secure wireless network for Odessa College owned equipment. It has full access to the internal network.

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, AD-HOC wireless PC to PC connections, etc.) All network hardware must be installed and secured by the IT division or its authorized agents.

Unauthorized Servers: Software that creates a server for use over the network via a url, ip address, or file share is 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.

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, FrostWire, Bear share, Vuze, 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.
- Use of any program that allows a user to connect to their PC from the internet which does not require the use of Odessa College's VPN service is prohibited. (I.e. Gotomypc.com etc.)
- Use of password cracking utilities to gain access to password protected (internal or external) data is prohibited.

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.
- Use of third party products to mass email students, faculty, or staff of Odessa College is prohibited. All users are required to use products which are approved and provided by the IT Division.

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.

Use of Computer Resources Policy – Employee Acknowledgment Section

I have read the terms and conditions of the Odessa College Use of Computer Resources Policy and agree to each and all of them.

Sign your Name: _____

Print your Name: _____

Signature Date: _____