OCC BOARD POLICY ON APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES AND ASSOCIATED PROCEDURE (3.8.2)

POLICY

DIVISION III BUSINESS SERVICES

3.8 INFORMATION TECHNOLOGIES

3.8.2 Appropriate Use of Information Technology Resources

Information technology resources (computers, voice and data networks, electronic data and information) are provided by Oakland Community College to its faculty, administration, and students in support of the college mission. Users of the information technology resources will abide by applicable Federal and State laws and the college's regulations (Technology Appropriate Use Regulations) governing the use of these resources, and will use them in support of activities directly related to duties and assignments.

Initial Approval: 1/26/89

Public Act: Federal Copyright Law Title 17, Paragraph 117 (revised 7/1/85).
Federal Computer Fraud Abuse Act
Federal Electronic Commission
Privacy Act.
Michigan Computer Law, Section 174 of P.A. 328, 1931, as amended.

Revised: 04/21/03

PROCEDURE

3.8 INFORMATION TECHNOLOGIES

3.8.2 Appropriate Use of Information Technology Resources

Information technology resources (computers, voice and data networks, electronic data and information) are provided by Oakland Community College to its faculty, administration, and students in support of the college mission. This document outlines the appropriate use of college information technology resources. More detail may be found in the Technology Appropriate Use Regulations.

A. ACCESS TO COMPUTER SYSTEMS AND NETWORKS

College employees may receive user accounts based on the requirements of their job. Students enrolling in courses which require user accounts are provided them for the terms enrolled in those courses.

B. STANDARDS OF CONDUCT

Users of OCC's computer systems and electronic networks agree to abide by applicable Federal and State information technology laws as well as the college's standards of conduct. This shall include, but not be limited to, any copyright protection of programs or files.

C. APPROPRIATE USE

Computer and network resources must be used in support of activities directly related to your duties or assignments at OCC. These activities include but are not limited to:

1. completion of assigned job duties or class assignments
2. relevant communication with colleagues at OCC and other institutions
3. exchange of research data and papers
4. authorized exchange of computer programs to support academic research, instruction, and administration, provided such exchange does not violate any copyright protection.

D. INAPPROPRIATE USE

Any use of computer and network resources for activities outside the college mission is inappropriate. These activities include but are not limited to:

1. unauthorized access to computer accounts or files
2. development or use of programs designed to monitor or damage data files
3. use of college resources to support the activities of any organization not so approved by the college administration
4. use of college resources for personal consulting, programming, or other profit or not-for-profit activities

5. use of electronic mail systems for personal attacks, offensive language, political or religious solicitations, or advertising for goods or services
6. disclosure of passwords or other data which might allow unauthorized persons to gain access to computer accounts, files, or electronic mail.

E. VIOLATIONS

Any user who perceives that college information technology resources are being used in violation of the standards outlined in this document should report the incident, in writing, to the appropriate Dean or other responsible administrator. If it is deemed necessary, Information Technologies will work with the OCC Human Resources and/or Public Safety Departments to investigate any misuse of computer resources. Any employee or student found to have violated college standards of conduct will be subject to disciplinary action up to and including discharge or dismissal from the college. Any suspected violation of State or Federal information technology laws will be reported to the appropriate legal authority for investigation.

OAKLAND COMMUNITY COLLEGE

Technology Appropriate Use Regulations

INTRODUCTION

Oakland Community College's **Technology Appropriate Use Regulations (TAUR)** is a body of standards of behavior that is intended to promote the responsible use of electronic communications and to prevent the abuse of computers and network systems. The TAUR identifies uses of technology that are appropriate, inappropriate, or illegal. These regulations and standards of behavior apply to all faculty, students, staff and College-registered organizations.

All regulations are subordinate to the technology policies of the Oakland Community College Board of Trustees, attached at the end of this document.

Appropriate uses of technology are those which facilitate communication among those conducting College business, support the function of College systems, and otherwise further OCC's Mission, Goals and Vision.

Inappropriate uses of technology are those which violate the function of College business by harming or interfering with the work of others or by engaging in illegal acts. The TAUR makes it a violation "to recklessly or maliciously interfere with or damage, in violation of College rules, computer or network resources or computer data, files, or other information." The TAUR also makes it clear that "misappropriation of data or copyrighted materials, including computer software, may constitute theft."

Further definition of Appropriate and Inappropriate Use appears in OCC Board Policy 3.8.2.

College owned or operated computing resources are for the use of faculty, students, staff and other authorized individuals. Individuals should exercise responsible, ethical behavior when using these facilities. The College does not attempt to articulate all required or proscribed behavior by its users. Therefore, each individual's judgment on appropriate conduct must be relied upon. The basic premise is that legitimate use of a computer or network does not extend to whatever an individual is capable of doing with it. Just because individuals are able to circumvent restrictions or security doesn't mean that they are allowed to do so.

The College has the right, but not the duty, to monitor any and all aspects of its network, including, but not limited to, monitoring sites individuals visit on the Internet, monitoring chat groups and newsgroups, monitoring social networking sites or mobile applications accessed using the College's network, reviewing material downloaded or uploaded by individuals, and reviewing email sent and received by individuals. All users should be aware that the IT System Administrators perform periodic security checks of the College network and attached components. These checks include password scanning, virus detection, file system/directory use and hardware and software inventory probes. OCC extends to its student, faculty, and staff a reasonable expectation of privacy in electronic communications. However, the privacy of electronic communications and documents cannot be guaranteed by the College. Users of the network give a limited waiver of any right to privacy in material created, stored, sent or received via the College's network; this limited waiver constitutes consent by the user to any and all such monitoring and security checks and measures as OCC, in its reasonable discretion, determines are appropriate to protect the network and its community of users.

Disclaimer of Liability

The College will not be responsible for any damages, direct or indirect, arising out of the use of its Internet, computing or telecommunication resources.

VIOLATIONS

Alleged violations of the types below should be reported directly to the appropriate Dean or other responsible administrator or to the police if the situation is potentially serious or requires immediate attention. If the person responsible is not affiliated with the College or if it is not possible to identify the individual, the incident can still be reported. Save electronic copies of all correspondence for evidence.

Violations of these Regulations or the OCC Board Policy on Information Technologies will be subject to consequences consistent with Board Policy 3.8.2.E, "Violations", and this Regulation. The College reserves the right to audit and/or suspend without notice the electronic communications of any user pending the results of an inquiry into a suspected violation of TAUR or the law. Users in suspected violation of TAUR may lose their right to access College electronic communications. Consequences of inappropriate use may include, but are not limited to: the immediate removal from online information systems of material that is believed to infringe TAUR or the law; reporting of suspected violations to appropriate law enforcement authorities; and action by the Dean or another responsible administrator within the College's disciplinary framework potentially resulting in discharge or dismissal from the College.

All of the activities listed as violations below are examples of prohibited conduct. However, the list is not comprehensive. Some of the conduct identified as violations of the TAUR is also illegal.

ACCESS

- **Unauthorized access**
  As stated in the **TAUR**, legitimate use of a computer or network does not extend to whatever an individual is capable of doing. In some cases, operating systems have security holes or other loopholes that people can use to gain access to the system or to data on that system. This is considered unauthorized access. If someone inadvertently turns on file sharing on their personal computer, you do not have the right to read or delete their files unless you have been given explicit permission from the owner. This is much like accidentally leaving your house door unlocked. You wouldn't expect a burglar to use that as an excuse for robbing you.

- **Unauthorized use of College resources** (e.g. using someone else's dial-in access or borrowing their OCC ID and password to access College systems).

- **Unauthorized use by sharing OCC IDs and passwords** (unauthorized use). Your OCC ID and password are provided for your personal use only. OCC IDs provide access to a wide range of services that are restricted for personal use you (such as grades, address information, registration bill, salary, benefits) or are restricted for use by the College community (such as e-mail, remote dial-in, library services, Internet access, news, chat). If you share your OCC ID with a spouse, family members, friends or others, then you are giving them access to services they are not authorized to use. They will also have access to all of your personal information. They may even embarrass you by posting to a news group in your name or by posing as you in a chat session or e-mail.

  Obtaining, possessing, using or attempting to use someone else's password regardless of how the password was obtained (e.g. password sharing).

  DO NOT SHARE YOUR PASSWORD WITH ANYONE. If you suspect that someone may have discovered your password, change it immediately and/or notify the OCC IT Call Center.

  DO NOT USE ANYONE ELSE'S PASSWORD. Using someone else's password to access services or data is also a violation of policy regardless of how the password was obtained. (PERIOD/DOT/ZERO Tolerance)

- **Accessing, or attempting to access, another individual's data or information without proper authorization** (e.g. using another's OCC ID and password to look at their personal information).

- **Sending forged messages under someone else's OCC ID** (e.g. sending hoax messages, even if intended to be a joke).

- **Unauthorized Encryption Prohibited.**
  The use of any unauthorized encryption technology which hinders the ability of the College to access data on any College computer system or network is prohibited.

INTERFERENCE
Interfering with Activities of Others
This can be any activity that disrupts a system and interferes with other people's ability to use that system. In some cases, consuming more than your "fair" share of resources can constitute interference. Some examples are:

- E-mail bombing that causes a disk to fill up, the network to bog down, or an e-mail application to crash.
- Taking advantage of a net split to take over a chat channel and then kicking off or blocking other users.
- Posting many messages to a single news group or mailing list making it difficult for subscribers to carry on their normal discussion.
- Flooding a chat channel with a continuous stream of messages so that it disrupts the conversation.

- Attack methods not limited to spoofing, snow shoeing, phishing, pharming, or “other malicious behavior”.

Denial of service attacks will be treated as a direct intrusion to the College network, and offenders will be prosecuted by the College.

- **Releasing a virus, worm or other program that damages or otherwise harms a system or network.**

- **Preventing others from accessing services** (e.g. taking over a chat channel and kicking other users off).

- **E-mail Bombing (sending a crippling number of files across the network)**
  Flooding someone with numerous or large e-mail messages in an attempt to disrupt them or their site is know**n** as "e-mail bombing." Often this is done to retaliate because someone has done something annoying. But more often than not, e-mail bombing will either cause problems for your local system or disrupt service for thousands of other innocent bystanders. If you are having a problem with someone, pursue an acceptable method to report the situation.

- **Impeding, interfering with, impairing, or otherwise causing harm to the activities of others** (e.g. propagating electronic chain mail or sending forged or falsified e-mail).

- **Chain E-mail and Virus Hoaxes**
  The most important thing to remember if you get chain e-mail is do not help propagate it. Chain e-mail usually contains phrases like "pass this on," "forward - do not delete," "don't break the chain," "this is safe, don't worry," "let's see how long this takes to get back to the start," "this has been around the world 20 times," "7 years of good luck!," "I don't wanna die," "your mom would want you to do this," etc. Often, there is some story about how lucky a person has been since they forwarded the chain e-mail or how unlucky they were because they didn't. Sometimes chain e-mail is disguised. It tells of some kid who is dying and wants post cards, or it warns about e-mail viruses or internet shutdowns. Don't fall for it. It's all chain mail, and it's designed to get you to forward it.

  In recent years, chain mail **hoaxes** of various sorts have become widespread on the Internet. Some are virus warnings like "Good Times," "PenPal," and "Irina." Others are like the "Naughty Robot" that claims to have all your credit card numbers. They tell you to forward the "warning" to everyone you know. Most hoaxes start out as pranks but often live on for years, getting passed around by new people who have just joined the Internet community. Don't believe every warning you get via e-mail. You should not pass these warnings on unless you verify the authenticity. You should contact the OCC IT Call Center, or check out one of the many sites on the Internet that track hoaxes:

  - CIAC
  - Computer Virus Myths
  - National Fraud Information Center

If you get chain e-mail from someone with an OCC e-mail address, you should report it. If you get chain e-mail from someone not affiliated with OCC, you can reply to the sender and let them know you are not happy about getting chain e-mail from them, or you can delete and ignore it.

WRONGFUL USE

- **Tapping phone or network lines (e.g. running network sniffers without authorization)**
  Running a network "sniffer" program to examine or collect data from the network is considered tapping a network.

- **Unauthorized access to data or files even if they are not securely protected** (e.g. breaking into a system by taking advantage of security holes).

- **Commercial Use of College Resources**
  Using e-mail to solicit sales or conduct business, setting up a web page to advertise or sell a service, or posting an advertisement to a news group all constitute commercial use. Even if you use your own personal computer, but you use the College’s network, you are in violation of the regulations.

- **Export Restrictions**
  Because of United States export restrictions, programs or files containing encryption technology are not to be placed on the Internet via College access or transmitted in any way outside the United States without prior written authorization from the IT Department.

- **Forgery**
  Altering electronic communications to hide your identity or impersonate someone else is considered forgery. All e-mail, news posts, chat sessions or any other form of communication should contain your name and/or OCC ID. Forgery includes using another person's identity or using an identity that's fake (like god@heaven or anon@nowhere). Forgeries intended as pranks or jokes are still considered violations.

- **Downloading or posting to College computers, or transporting across College networks, material that is illegal, proprietary, in violation of College contracts or otherwise is damaging to the institution** (e.g. launching a computer virus, distributing child pornography via the web or posting a College site-licensed program to a public bulletin board)

- **Using College resources for unauthorized purposes** (e.g. using personal computers connected to the campus network to set up web servers for illegal, commercial or profit-making purposes).

HARASSMENT

Electronic communication that is repeated and unwanted may constitute harassment. In general, communication targeted at a specific individual with the intent to harass or threaten is a violation of OCC policy. If you receive unwanted e-mail or other form of communication, you may want to consider notifying the sender that it is unwanted. Many times a person will not realize that their communication is unwanted unless you tell them. If the sender continues to communicate after being placed on notice, or if you feel uncomfortable confronting the sender, the incident should be reported.

- **Harassing, threatening, cyberbullying, or otherwise causing harm to specific individuals** (e.g. sending an individual repeated and unwanted {harassing} e-mail or using e-mail social networking sites or mobile applications to threaten or stalk someone).

- **Harassing or threatening classes of individuals.**

ILLEGALITIES

Everything listed under the "Illegal under State and Federal Laws" (at the end of the TAUR) is a violation of College policy. This is not a comprehensive list, but it contains the activities most frequently asked about.

Illegal Under State and Federal Law

- **Child Pornography**
  Child pornography, material that depicts minors in a sexually explicit way, is illegal.

- Under the federal child pornography statute (18 USC section 2252), anyone under the age of 18 is a minor. Individual states also have child pornography statutes and the age of minority varies by state. **Knowingly uploading or downloading child pornography is a federal offense**. It is also illegal to advertise or seek the sale, exchange, reproduction or distribution of child pornography. Lewd exhibition of genitals can constitute sexual conduct and therefore, any graphic files containing images of naked children could violate the federal child pornography statute.

- **Distribution of Pornography to Minors**
  Possession of non-obscene adult pornography is legal, but it is illegal to distribute to minors.

- **Obscenity**
  Obscenity is illegal. Virtually every state and municipality has a statute prohibiting the sale and distribution of obscenity, and the federal government prohibits its interstate transportation. The Supreme Court in Miller v. California, 413 U.S. 15, (1973), narrowed the permissible scope of obscenity statutes and applied this three part test to determine constitutionality: (a) whether the average person applying contemporary community standard would find the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined in applicable state law; and (c) whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.

- **Scams and Pyramid Schemes**
  Beware of money-making "opportunities" on the Internet. A common scam is the pyramid scheme. You get an e-mail message with a subject like "MAKE MONEY

FAST" and it instructs you to send money to the people on the list, add your name to the bottom of the list and send it on to some number of people. At OCC, this is considered chain mail, but it is also illegal under 18 U.S.C section 1302. The US Postal Service and the Federal Trade Commission provide information to help individuals identify scams and report them. Pyramid schemes that use US Postal mail to send money are considered mail fraud and can be reported to the USPS.

- **Copyright Infringement**
  Almost all forms of original expression that are fixed in a tangible medium are subject to copyright protection, even if no formal copyright notice is attached. Written text (including e-mail messages and news posts), recorded sound, digital images, and computer software are some examples of works that can be copyrighted. Unless otherwise specified by contract, the employer generally holds the copyright for work done by an employee in the course of employment.

  Copyright holders have many rights, including the right to reproduce, adapt, distribute, display and perform their work. Reproducing, displaying or distributing copyrighted material without permission infringes on the copyright holder's rights. However, "fair use" applies in some cases. If a small amount of the work is used in a non-commercial situation and does not economically impact the copyright holder, it may be considered fair use. For example, quoting some passages from a book in a report for a class assignment would be considered fair use. Linking to another web page from your web page is not usually considered infringement. However, copying some of the contents of another web page into yours or use of video clips without permission would likely be infringement.

  - **Software Piracy**
    Unauthorized duplication, distribution or use of someone else's intellectual property, including computer software, constitutes copyright infringement and is illegal and subject to both civil and criminal penalties. The ease of this behavior on-line causes many computer users to forget the seriousness of the offense. As a result of the substantial amounts of money the software industry loses each year from software piracy, the software companies enforce their rights through courts and by lobbying for, and getting, stiffer criminal penalties. It is a felony to reproduce or distribute ten illegal copies of copyrighted software with a total value of $2,500 within a 180-day period. Penalties for a first time felony conviction of software piracy include a jail term of up to ten years and fines up to $250,000.

  - **Sound Recording Piracy**
    Another form of copyright infringement is the unauthorized duplication and distribution of sound recordings. Online piracy is increasing as many people use the Internet to illegally distribute digital audio files (e.g. MP3 format). The Recording Industry Association of America (RIAA) daily monitors the Internet and scans for sites that contain music. They have been successful in getting the sound recordings removed from those sites.

    Federal copyright law grants the copyright owner in a sound recording (typically, a record company) the exclusive right to reproduce, adapt, distribute, and in some cases, digitally transmit their sound recordings. Therefore, the following activities, if unauthorized by the copyright owner, may violate their rights under federal law:

- Making a copy of all or a portion of a sound recording onto a computer hard drive, server or other hardware used in connection with a web site or other online forum. This includes converting a sound recording into a file format (such as a .wav or mp3 file) and saving it to a hard drive or server;
- Transmitting a copy or otherwise permitting users to download sound recordings from a site or other forum; and/or
- Digitally transmitting to users, at their request, a particular sound recording chosen by or on behalf of the recipient.

If you reproduce or offer full-length sound recordings for download without the authorization of the copyright owner, you are in violation of federal copyright law and could face civil as well as criminal penalties. **Placing statements on your web site, such as "for demo purposes only," or that the sound files must be "deleted with 24 hours," does not prevent or extinguish this liability.**

There are several entities you may need to contact before you can use recorded music online. First, you should understand that the copyright in a sound recording is distinct from the copyright in the recording's underlying musical composition. Thus, even if you have secured the necessary licenses for publicly performing musical compositions (from, for example, ASCAP, BMI and/or SESAC) or for making reproductions of musical compositions (from, for example, the Harry Fox Agency), these licenses only apply to the musical composition, not the sound recording. Licenses to use particular sound recordings must be secured from the sound recording copyright owners -- generally the record company that released the recording.

Federal Computer Security Violations

The primary federal statute regarding computer fraud, 18 U.S.C section 1030 is the “Computer Fraud and Abuse Act” (CFAA) was updated in 2001 by the USA Patriot Act and by the Identity Theft Enforcement and Restitution Act in 2002 and 2008 to protect computer and data integrity, confidentiality and availability. In addition to the federal statute is the Michigan statute Act No. 566; Public Act of 2006 effective January 2, 2007 as an amendment to 2004 PA 452. Examples of violations are:

- Theft of information from computers belonging to financial institutions or federal agencies, or computers used in interstate commerce;
- Unauthorized access to government computers;
- Damage to systems or data (intentionally or recklessly);
- Trafficking in stolen passwords; and/or using computing resources to perpetrate an act of terror
- Extortionate threats to damage computers.

- **Bomb Threats and Hoaxes**
  It is illegal to send a message via e-mail that threatens other persons or property. While this might seem obvious, every year a number of individuals send what they believe are "hoax messages." Such messages may be investigated by federal authorities with the result that the senders end up with their names in the files of the FBI and/or CIA. This is not an exaggeration!

  It also violates OCC's **TAUR** to send certain kinds of hoax messages (for example, April Fool's jokes that appear to be from a professor or some other College official). Such hoaxes constitute forgery and will be referred for appropriate disciplinary action.