Copyright Infringement Policies and Sanctions

Table of Contents

Copyright Infringement Policies and Sanctions (Including Computer Use and File Sharing)

Any sharing of copyrighted material without proper licensing or permission from the owner/author/software manufacturer is prohibited by law, and is not condoned Sacramento Ultrasound Institute. Any students accused of copyright violation or infringement will be required to resolve matters on their own without involvement from SUI. Additionally, all students are subject to SUI's Guidelines for Responsible Computing and subject to disciplinary action should those policies be violated. (See Page 3)

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please visit the U.S. Copyright Office Web site, especially the FAQs section.

Acceptable Use Policy

Introduction

This policy governs the management of SUI's computer data networks as well as stand-alone computers that are owned and/or administered by SUI. The policy reflects the general principles of SUI's community and indicates, in general, what privileges and responsibilities are characteristic of the SUI's computing environment.

Terminology

A number of terms used below have specific meanings in the context of this document. We define them here:

- Network – The complete mechanism by which computers and peripherals are connected.
- Networked computer – A computer system that is connected to any data network maintained by SUI.
- Shared computing resource – A networked computer and SUI peripherals that can be used by more than one person.
- Central – Refers to networked computers and peripherals purchased, maintained, and operated by SUI and made available to all or part of the SUI's community.
- Department – Refers to networked computers and peripherals purchased, maintained, and operated for academic-specific purposes by individual academic departments and made available to those associated with the program the resources support.
- Individual – Refers to networked computers purchased for use by an individual member of SUI's community, and which can be made available to other individuals or groups by the owner.
- System administrator – The person having executive authority over one or more networked computers.
- Clients – members and/or guests of SUI for whom the services and resources of SUI are provided.
- Distributed resources – applications and services (enterprise-wide and program specific) that are provided to members and/or guests of SUI for academic, communication and social networking purposes.

General Policies

Computer and network use has become an essential part of many SUI activities. While much computing is now done on individually controlled computers (personal computers, workstations, etc.) most information sources and communications systems reside on shared, central computers, or use shared networks. Distributed resources, such as public access workstations provide additional computing tools. SUI, together with computing resources throughout campus has the responsibility of providing and maintaining shared computing tools. General policies regarding the resources SUI provides are outlined below:

- Access – SUI will provide access to appropriate central and campus computing resources, and to networks, for all members of the SUI community whose studies and work requires it.
- Availability – SUI will make campus computing resources and networks available to the SUI community with the fewest interruptions possible.
- Monitoring - SUI maintains logs of various activities associated with computer usage on campus (i.e. URLs visited, intrusion logs, email logs, etc). These logs are only used to manage the network traffic and are not to be used to infringe upon the privacy of network clients.
- Interception - To protect the SUI community from email viruses and other threats to the network, may intercept messages that meet specific criteria indicating the presence of a threat, informing the SUI community as soon as reasonably possible. SUI will not open any intercepted messages without the permission of the recipient.
- Archiving – SUI regularly archives (back-ups) material on enterprise servers. Information is preserved for a finite period and may be used to recover lost or corrupted data. Clients should be aware that these backup tapes contain a record of all files, including email and network logs, on the system at the time of the backup.

Security

Sacramento Ultrasound Institute will assist clients of central and campus shared computing resources in protecting information they store on those resources from accidental loss, tampering, or unauthorized search, or other access. Appropriate information on the security procedures implemented on all resources will be made available by the system administrator. Clients should be aware, however, that unauthorized individuals might gain access to electronic communications and files. Clients who are concerned about maintaining the privacy of their email and files are encouraged to install personal security applications or password protect all documents and data stored on hard drives.

In the event of an inadvertent or non-malicious action resulting in the loss of or damage to that information, or the invasion of the user's privacy, SUI will make reasonable efforts to mitigate the loss or damage. SUI will provide reasonable security procedures on SUI-maintained systems. Clients are responsible for properly maintaining the protections under their control, specific to files associated with their computer accounts. Clients may request that arrangements be made to protect information stored on such resources. These requests will be honored at the discretion of the manager of the resource.

The user is responsible for correct and sufficient use of the tools each computer system provides for maintaining the security and confidentiality of information stored on it. For instance:

- Computer accounts, passwords, and other types of authorization are assigned to individuals and should not be shared with others.
- Individuals should select and obscure the account password and change it frequently.
- Individuals should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive information.
- All individuals should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting conduit for attacks.

Other Resources

System administrators of departmental and individual computing resources are responsible for the security of information stored on those resources, for making appropriate information on security procedures available to clients of those systems, and for keeping those systems free from unauthorized access.

Confidentiality

Sacramento Ultrasound Institute intends that all files and email are private and confidential unless the owner intentionally makes this information available to other groups or individuals. Interception of network transmission is strictly forbidden. In general, information stored on computers is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes this information available to other groups or individuals. Sacramento Ultrasound Institute will assume that clients wish information they store on central and shared computing resources to remain confidential. SUI will maintain confidentiality of all information stored on their computing resources. Similarly, privileged information on account usage (in other words, that available only to clients with system privileges) will also be treated with confidentiality. Privileged information available to system administrators will be held in confidence.

The administrator of the computer system involved will review requests for disclosure of confidential information. Such requests will be honored only when approved by SUI officials authorized by appropriate policy or procedures, or when required by local, state, or federal law.

Censorship

Free expression of ideas is central to the academic process. Therefore, SUI's computer system administrators will not evaluate any information from individual accounts unless it is determined that:

- The presence of the information involves an illegality (e.g., copyrighted material, software used in violation of a license agreement).
- The information in some manner endangers computing resources or the information of other clients (e.g., a computer worm, virus, or other destructive program).
- A SUI judicial or grievance process finds cause for content to be removed in accordance with standing policies and procedures.

SUI computer systems administrators and department computer systems administrators may remove from central or department computers information as defined above. Clients whose information is removed will be notified of the removal as soon as is feasible. Clients wishing to appeal such removal of information may do so in accordance with the appropriate appeals process relative to their status within SUI.

Responsibilities of the User

Access to computing resources and networks is a privilege to which all SUI faculty, staff and students are entitled. Access may also be granted to individuals outside SUI for purposes consistent with the mission of SUI. Certain responsibilities accompany that privilege; understanding them is important for all computer clients. Refer to the section 'Sanctions' regarding the policy of Sacramento Ultrasound Institute in handling infractions of these responsibilities. These responsibilities are listed below:

Institutional Purposes

Use of SUI's computing resources and networks is for purposes related to the SUI's mission of creativity and artistic expression; academic teaching, learning and research; and community engagement. The use of computing resources and networks are for purposes related to an individual's studies, instruction, or the discharge of duties as employees, their official business with SUI, or their other SUI-sanctioned activities. The use of SUI's computing resources, networks, or bandwidth for commercial purposes is not permitted except by special arrangement with appropriate computing systems administrators and other appropriate SUI officials.

Legal Usage

Computer resources and network access and bandwidth may not be used for illegal purposes. Examples of illegal activities include:

- Intentional harassment of others.
- Intentional destruction of or damage to equipment, software, or data belonging to Sacramento Ultrasound Institute or other clients.
- Intentional disruption or unauthorized monitoring of electronic communications.
- Unauthorized acquisition of and/or distribution of copyrighted and/or licensed material.

Ethical Usage

Computing resources and network access should be used in accordance with the standards of SUI community as described in such documents as the Student Handbook and Faculty Handbook. Examples of unethical use follow; some of them may also be illegal:

- Violations of computer system security.
- Unauthorized use of computer accounts, access codes, or network identification numbers assigned to others.
- Intentional use of computer communications facilities and resources in ways that unnecessarily impede the computing services available to others (randomly initiating interactive electronic communications or email exchanges, overuse or interactive network utilities, etc.).
- Use of computing facilities for private business purposes unrelated to the mission of the SUI or campus life.
- Academic dishonesty (plagiarism, cheating).
- Violation of software license agreements.
- Violation of network usage policies and regulations.
- Violation of others' right to privacy.

Collegial Usage

Individuals using Sacramento Ultrasound Institute computing resources can facilitate computing in SUI's environment in many ways. Respecting the diversity of the user community demands the practice of responsible computing. This should include:

- Regular deletion of unneeded files from one's accounts on shared servers.
- Refraining from overuse of connection time on public access machines, information storage space, printing facilities, or processing capacity.
- Refraining from overuse of interactive network utilities.
- Refraining from overuse of network-shared bandwidth.

Sanctions

Sacramento Ultrasound Institute treats the abuse of computing facilities, equipment, software, data, networks, or privileges seriously. Unauthorized access to electronic communications and files is strictly forbidden. Use of computing resources is to be conducted in keeping with the guidelines established in the following official publications of SUI: this Catalog, the Faculty and Student Handbooks. Sanctions adjudicated by Sacramento Ultrasound Institute will be resolved in the manner stated in the appropriate handbooks and policies applicable to the status of the individual user. Illegal acts involving Sacramento Ultrasound Institute computing resources may also be subject to prosecution under local, state, and federal laws.

Adopted December 2015