



PERSONAL COMPUTING TIPS FROM THE UC WASHINGTON CENTER

The UC Washington Center is an island removed by distance and time from the other campuses of the University. The Center's network resources are our connection back to the home campuses. We all share these resources and share in the responsibility for making sure that they are available to one another. Our actions can affect the availability of this resource for everyone else.

ACCEPTABLE USE POLICY

The use of information technology resources at the Center is governed by the University of California's Electronic Communications Policy (see <http://www.ucop.edu/ucophome/policies/ec/>), related University Business & Finance bulletins and local policies established by the UC Washington Center. Below are various Center policies governing the acceptable use of its network and other information technology resources.

COPYRIGHT

Theft of copyright is a crime! Theft of copyright is the illegal reproduction of any materials protected by U.S. copyright laws including but not limited to, music files, software, and video; or violation of the terms of applicable software licensing agreements.

- If you haven't paid for it, don't download pictures, music, videos, software, etc. labeled with a copyright notice.
- If it doesn't have a copyright notification, still assume that it is copyrighted unless it specifically says that it is not.
- If you think that you may have unlawfully attained copyrighted materials on your computer, removed them immediately.
- For additional information about the University's policy on copyright see the UC Policy on Copyrighted Materials at <http://www.ucop.edu/irc/policy/copyright.html>.

PEER-TO-PEER FILE SHARING

The use of peer-to-peer file sharing software such as kazaa, gnutella, netdonkey, e-mule, bittorrent and the like is prohibited. This software can be used to download copyrighted movies, music, software and other files without permission.

- It can consume inordinate amounts of the network resources shared by all.
- It can consume inordinate amounts of memory and hard drive space on your personal computer causing it to slow or even stop.
- It can increase your computer's vulnerability to infection by malware (viruses and spyware).
- The failure to adhere to this policy can result in frequent interruptions in shared network service.

MALWARE

'Malware' is a catch-all term for viruses, computer worms, spyware and other malicious software. The creators of malware are very sophisticated and can be nasty in their attacks. The Center requires all network users to install anti-viral and anti-spyware software on their computers and to keep this software up-to-date. It is strongly recommended that this software be installed in advance of arrival at the Center.

Antiviral software is available to students, faculty & staff without charge though the following sites:

- Berkeley (<http://software.berkeley.edu/index.html>)
- Davis (<http://scg.ucdavis.edu/protect.cfm?=item4>)
- Irvine (<http://www.security.uci.edu/desktop/anti-virus.php>)
- Los Angeles (<http://www.bol.ucla.edu/software/sophos/>)
- Riverside (<http://cnc.ucr.edu/security>)
- San Diego (<http://software.ucsd.edu/resourcefiles/studentsophos.html>)
- Santa Barbara (<http://www.lsit.ucsb.edu/kb/idx/41/049/article/>)
- Santa Cruz (<http://security.ucsc.edu/antivirus.shtml>)
- Other users may take advantage of no charge software available at:
http://www.avast.com/eng/avast_4_home.html

You can download a basic, no-charge anti-spyware tool at
<http://www.microsoft.com/athome/security/protect/windowsxpsp2/Default.mspx>.

OTHER PROHIBITED ACTIVITES

For your referral, a list of other activities that are violations of University and/or Center policy and are prohibited is listed below:

1. Using a computer account without authorization.
2. Obtaining a username and/or password without consent of the account owner.
3. Employing a false identity (the name or electronic identification of another). Pseudonyms (an alternative name or electronic identification for oneself) are allowed for privacy or other reasons, so long as the pseudonym clearly does not constitute a false identity.
4. Connecting a personal wireless network hub to the Center's network.
5. Using the Center's network to gain un-authorized access to any computer system.
6. Attempting to monitor or tamper with another's electronic communications; this includes reading, copying, changing or deleting another user's files or software without the explicit agreement of the owner.
7. Attempting to circumvent data protection schemes or uncover security loopholes.
8. Knowingly performing an act that will interfere with the normal operations of computers, peripherals, network or other technology infrastructure at the Center. This includes running or installing on any computer system, network or other technology infrastructure at the Center (or giving another user) a program intended to damage or place excessive load on a computer, network or other technology system.
9. Deliberately wasting the Center's technology resources or excessive consumption of network resources. This includes knowingly sending or forwarding chain letters or unsolicited e-mail ("Spam").
10. Using the Center's network or University-owned equipment for unlawful purposes.
11. Using the University network or University-owned equipment for commercial gain.

ABUSE OF NETWORK OR TECHNOLOGY RESOURCES

In the event of abuse of network resources, including theft of copyright, inordinate consumption of network resources or utilization of network resources and/or other behavior that is detrimental to the operation or integrity of the Center's network, the Center may take the following actions:

1st offense

1. Immediate termination of network access for offending computer(s) or other network attached devices;
2. Violator will be notified as to steps required to restore network access;
3. Violator has three business days from issuance of violation notification to respond to the UC Washington Center Information Services staff that all appropriate actions required by the violation notification have been performed. These action may include but are not limited to:

- a. In the case of theft of copyright the owner of a personally-owned computer must inform UC Washington Center Information Services in writing:
 - i. that the offending material has been removed;
 - ii. and that the violator has ceased engaging in this activity.
- b. In the case of consumption of inordinate amounts of network resources or other misuse of network resources the owner of a personally-owned computer must inform UC Washington Center Information Services in writing:
 - i. that appropriate anti-viral and anti-spyware software is installed on the computer with recently updated definitions for this software and that this software has scanned and successfully removed all viruses and spyware;
 - ii. has ceased all behavior that is detrimental to the operation or integrity of the Center's network;
 - iii. and, as applicable, has removed file sharing or other offending software.

Failure to comply or a 2nd violation

1. Permanent termination of network access for offending computer(s) or other network attached devices and Center network user account(s);
2. \$100 fine payable to the UC Regents;
3. And may result in additional residential disciplinary action and/or cancellation of violator's housing contract;
4. Upon issuance of failure to comply notification or 2nd violation, violator has one business days from issuance of violation notification to respond to the notification;
5. In the case of theft of copyright or other illegal activity, the violator is also potentially subject to legal action by the copyright holder regardless of any actions that the University may take.

If you have questions about computing resources at the Center, please contact support@ucdc.edu. Thank you!