

# Institutional Policy: Use of College Electronic Communication Services

Palmer College of Chiropractic provides telephone, voice mail, facsimile, computer, software, network and Internet services to employees and students as resources to enable them to carry out their respective duties and responsibilities as well as to enhance the educational process. Employees and students shall exercise sound professional judgment when using these resources and shall not use any of these resources in a manner that is prohibited by College policy and procedures or by applicable laws.

## SCOPE

This policy applies to the entire College community and 3rd parties.

## DEFINITIONS

N/A

## ADMINISTRATIVE RULES

### College Property

Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the College and are not the property of users of the electronic communications services.

### Appropriate Use of Computer Networks

Electronic communications systems generally must be used only for activities to support and enhance the educational objectives of the college. All members of the College community and relevant 3rd parties (hereafter referred to as “Users”) are responsible for exercising good judgment regarding the reasonableness of personal use. Incidental personal use is permissible so long as:

- > It does not consume more than a trivial amount of resources.
- > It does not interfere with employee productivity.
- > It does not preempt any business activity.

Users are individually responsible for appropriate use of all assigned resources, including the computer, the network address or port, software and hardware.

## No Expectation of Privacy

The College does not guarantee that electronic communications will be private. Users should be aware that electronic communications could potentially be forwarded, intercepted, printed, and stored by others.

Users should have no expectation of privacy relating to their use of the computer network, including electronic mail.

## College Monitoring and Access

The College reserves the right to audit and/or monitor the use of computer systems including electronic mail, software and network services and Internet services it provides its users. While the College does not routinely monitor the content of electronic communications, such communications may be monitored and the usage of electronic communications systems may be monitored to support operational, maintenance, auditing, security, legal compliance and/or investigative activities. The College may intercept, access, read or disclose any communication created, received or stored using those resources.

The College shall follow all applicable laws regarding the monitoring, wiretapping, eavesdropping of recording of telephone conversations or the interception or opening of mail and shall not engage in those activities without good and sufficient cause.

## Statistical data

Consistent with generally accepted business practice, the College collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc.

Using such information, Information Services (IS) monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

## Authorization for Access

Employees and students may use only the computers, computer accounts, and computer files for which they have been authorized. You may not use another individual's account, a computer logged in with another users' account or attempt to capture or guess other users' passwords. Employees and students are strictly prohibited from gaining access to any computing files, records, communications or other information without proper authorization. Proper authorization must be obtained through the Information Services Department.

You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization.

## Passwords and Login information Management

Employees and students shall not share passwords or other confidential login information. Workstations, servers and network devices will be configured to:

- > Automatically expire passwords after ninety days when possible;
- > Lock out a user account after three invalid password attempts when possible; and
- > Prevent the reuse of at least two previous passwords when possible

Users are to follow these guidelines when selecting passwords:

- > Components of the user's name will not be used in any part of the password;
- > Dictionary words should not be used alone; and
- > Passwords must not be written down and left in obvious places such as: under a keyboard, on a monitor, calendar or desktop.

## Message Restrictions

Messages that are discriminatory, harassing, threatening, reflect negatively on the College or messages that are otherwise unlawful or inappropriate in an office environment, such as chain letters or unauthorized mass mailings are prohibited.

## Prohibited Uses of Computer Network

Employees and Students are expressly prohibited from using College computer networks or accessing the Internet from those systems for any of the following purposes:

- > External instant messaging;
- > External music and file sharing;
- > Copying or transmission of any document, software or other intellectual property protected by copyright, patent or trademark law, without proper authorization by the owner of the intellectual property;
- > Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing;
- > Political activities including sending political messages and solicitation of funds;
- > Gambling;
- > Viewing, downloading, or exchanging pornography;
- > Installing or downloading software that is not licensed to the College;

- > Illegal activities of any kind; and
- > Disclosure of Confidential Information without authorization.

## Copyrighted, Proprietary and Licensing Restrictions

The College complies with applicable laws and the licensing terms and conditions of the manufacturer pertaining to the use of computer hardware and software including, but not limited to copyright laws. Unauthorized use of licensed software is strictly prohibited. Employees and students shall not send or receive any copyrighted, proprietary or confidential information pertaining to the College without its prior authorization, and shall not send or otherwise distribute, any other copyrighted, proprietary or confidential information unless expressly permitted by applicable licenses or other agreements regarding the distribution of those materials.

## Prohibited software

Personal servers, such as (but not limited to) web, FTP, e-mail, chat, peer-to-peer, media (movies, music, etc.) sharing and Windows file sharing are not permitted. Programs used to evade, defeat or probe security measures, impede or disrupt operations are not permitted. Programs that impede desk-top computer operations, log key-strokes, create unusually high overhead, or otherwise impair the operation of a computer are not permitted. The use of remote control software must be approved by the Director of Information Services.

## Prohibited hardware

The use of dial-up modems is prohibited except for business purposes approved by Department of Information Services. Multiple Network Interface Cards (NICs) are prohibited to prevent simultaneous network connections, unless specifically authorized by the Director of Information Services. Hardware used to evade, defeat or probe security measures, impede or disrupt operations is not permitted.

## Electronic Mail

The following activities are prohibited:

- > Use of e-mail addresses for marketing purposes without explicit permission from the target recipient;
- > Forwarding of documents belonging to the College, or the contents of those documents, to individuals outside of the institution without having substantial institutional business purpose;
- > Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication;
- > Attempting to obtain or obtaining access to the email records or communications of others with no substantial institutional business purpose; and

- > Chain Letters/Chain E-mail.

To prevent the downloading of computer viruses, employees and students should not open e-mail attachments that are illegitimate or originate from an unknown or mistrusted source.

## Remote Access

Hardware or software intended to provide remote access to either the network or a desk-top computer is not permitted unless approved for use in writing by the Director of Information Services and configured according to procedures established by the Department of Information Services.

## Anti-virus measures

All computers connected to the network shall have a properly installed and updated anti-virus program. Anti-virus software provided by the College shall not be disabled or removed.

## Respecting Privacy Rights

Except as otherwise specifically provided, employees and students may not intercept or disclose or assist in intercepting or disclosing electronic communications. Confidential information must be removed from view, computer screens must be cleared and keyboards password locked when work areas are unattended.

## AMENDMENT OF POLICY

The College reserves the right to amend this policy from time to time as the interests of the College may require.

## STANDARD INSTITUTIONAL POLICY PROVISIONS

Institutional Policies are supplemented by provisions that are applicable to all institutional policies. It is the responsibility of all employees and students to know and comply with these standards.

[Standard Provisions Applicable to All Institutional Policies](#)

## ADDITIONAL INFORMATION

## ASSOCIATED PROCESSES AND/OR PROCEDURES

This policy may be supplemented by division or department-specific policies, processes, and/or procedures that describe policy implementation practices. Such supplemental procedures may be obtained from, referenced in, and/or linked from, the relevant division or department.

- > Process/Procedure (page 8, section 6.1)

## FORMS/INSTRUCTIONS

- > Need access to Administrative Systems?

Fill out a Computer Account Form, have it signed by your supervisor and the director of the department you are requesting data access for. Send it back to Information Services via inter-office mail or fax x5484. You will need Adobe Acrobat Reader to open and print this form.

- > Need a Student Computer Account?

Fill out a Student Computer Account Form. Students will need to fill out the form and bring it to Information Services in North Hall along with their Matric Number as well as an ID Card in order to set up the account

## CONTACTS

- > Palmer College of Chiropractic, Davenport IA Campus  
Mark Wiseley  
Senior Director of Information Services  
1000 Brady Street  
Davenport, IA 52803-5214  
(563) 884-5691 |  
[mark.wiseley@palmer.edu](mailto:mark.wiseley@palmer.edu)
- > Palmer College of Chiropractic, San Jose, CA Campus  
Kelly Goetz  
Network Manager, Information Services  
90 E. Tasman Drive  
San Jose, CA 95134-1617  
(408) 944-6104  
[kelly.goetz@palmer.edu](mailto:kelly.goetz@palmer.edu)
- > Palmer College of Chiropractic, Port Orange, FL Campus  
Matt Kellen  
Network Manager, Information Services  
4777 City Center Parkway  
Port Orange, FL 32129-4153  
(386) 763-2640  
[matt.kellen@palmer.edu](mailto:matt.kellen@palmer.edu)

- > Palmer College of Chiropractic, Davenport IA Campus  
Michelle Walker, M.S.  
Senior Director for Human Resources  
Office of Human Resources  
1000 Brady Street  
Davenport, IA 52803-5214  
(563) 884-5866  
[michelle.walker@palmer.edu](mailto:michelle.walker@palmer.edu)

## RELATED INFORMATION

- > N/A

## APPENDICES

- > N/A

## HISTORY

Last Revised: ..... February 2, 2010

Adopted: ..... N/A

Last Administrative Review: ..... November 4, 2009

Issuing Office:.....Office of Institutional Compliance  
Earlye Julien, PHR, M.S. Ed., CQIA  
Senior Director for Institutional Compliance & Chief Compliance Officer  
Palmer College of Chiropractic  
1000 Brady Street  
Davenport, Iowa  
Phone: (563) 884-5476  
Fax: (563) 884-5883  
[earlye.julien@palmer.edu](mailto:earlye.julien@palmer.edu)

Responsible Officer: .....Thomas Tiemeier, B.B.B., C.P.A.  
Vice Chancellor for Administration/Treasurer  
Palmer College of Chiropractic  
1000 Brady Street  
Davenport, Iowa  
Phone: (563) 884-5653  
[tom.tiemeier@palmer.edu](mailto:tom.tiemeier@palmer.edu)