Use of College Electronic Communication Services

Palmer College of Chiropractic (College) 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 Use of College Electronic Communication Services policy (Policy) applies to the entire College community, which is defined as including the Davenport campus (Palmer College Foundation, d/b/a Palmer College of Chiropractic), West campus (Palmer College of Chiropractic West) and Florida campus (Palmer College Foundation, Inc., d/b/a Palmer College of Chiropractic Florida) and any other person(s), groups, or organizations affiliated with any Palmer campus.

DEFINITIONS

For the purposes of this Policy, the following terms shall have the meanings specified below:

- The term **"College"** refers to Palmer College of Chiropractic, including operations on the Davenport campus; West campus; and Florida campus.
- The term **"College community"** refers to all students, faculty, staff (including administration), and any other person(s), groups, or organizations affiliated with any Palmer campus.

ADMINISTRATIVE RULES

College Property

Electronic communications systems and all files and 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:

1. It does not consume more than a trivial amount of resources.
2. It does not interfere with employee productivity.
3. 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 or 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 Technology (IT) 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. Employees and students 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 Technology Department.

Users should make a concerted effort to protect your passwords and to secure resources against unauthorized use or access. Users must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization. Additionally, it is the responsibility of all users to ensure that computer systems and the data which is accessed through them, are safe and secure. Systems should be placed in an area where it is not likely to be damaged and where the content of screens cannot be read by unauthorized people.

All employees will ensure that any printouts or other outputs from college systems are appropriately protected and disposed of when no longer needed. Printouts may not be copied, removed from the workplace, or shared with others without proper 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:

1. Automatically expire passwords after ninety days when possible;
2. Lockout a user account after five invalid password attempts when possible; and

3. Prevent the reuse of at least ten previous passwords when possible.

Employees and students are to follow these requirements when selecting passwords:

1. Passwords must be at least 8 characters in length;
2. Passwords may not be reused;
3. Passwords must not contain the user's Account Name or Display Name (Full Name);
4. Passwords must contain characters from three of the following four categories:
   a) Uppercase characters A through Z
   b) Lowercase characters a through z,
   c) Digits (0 through 9)
   d) Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and
5. 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.

Also, College systems must not be used for the creation, transmission, or deliberate reception of any images, data, or other material that is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene, or indecent. When communicating electronically, employees and students are expected to conduct themselves in an honest, courteous, and professional manner.

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:

1. External music sharing and file sharing;

2. 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;

3. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing;

4. Engaging in deliberate activities with consequences that may result in:

   a) Corruption or destroying other users' data,

   b) Using systems in a way that denies service to others (e.g. overloading the network), and/or

   c) Gaining access to systems in which users are not authorized;

5. Political activities including sending political messages and solicitation of funds;

6. Gambling;

7. Viewing, downloading, or exchanging pornography;

8. Installing or downloading software that is not licensed to the College;

9. Illegal activities of any kind; and

10. 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, email, chat, peer-to-peer, media (e.g. 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 desktop 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 Senior Director of Information Technology.

Employees: All software must be purchased, installed, and configured by the Information Technology department unless an alternative plan has been pre-approved by Information Technology; this includes all software packages, software upgrades, and add-ons, however minor. It also includes shareware, freeware, and any items downloaded from the Internet. Under no circumstances should any software be purchased or installed without the explicit agreement and/or approval of the Information Technology department.

Prohibited Hardware

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

Electronic Mail (Email)

Electronic mail (email) is a critical mechanism for business communication within the College. However, use of the Colleges' electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of the College.

Employees and students must use extreme caution when communicating confidential or sensitive information via email. Keep in mind that all email messages sent outside of the College become the property of the receiver. Employees and students should consider not communicating anything that they would not feel comfortable being made public. Employees and students should demonstrate particular care when using the "Reply All" command during email correspondence to ensure the resulting message is not delivered to unintended recipients.

The following activities are prohibited:

1. Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses);

2. Use of email addresses for marketing purposes without explicit permission from the target recipient;

3. 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;

4. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication;

5. Writing or presenting views on behalf of the College unless authorized to do so;

6. Intentional receipt and/or distribution of offensive, obscene, or pornographic material;

7. Attempting to obtain or obtaining access to the email records or communications of others with no substantial institutional business purpose; and

8. Chain letters/chain email; and

9. Sending any data unencrypted that contains HIPAA information, credit card information, Social Security numbers, or any other private or confidential information.

To prevent the downloading of computer viruses, employees and students should not open email 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 computer is not permitted unless approved for use in writing by the Senior Director of Information Technology and configured according to procedures established by the Department of Information Technology.

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.

College-owned computers will automatically receive a centrally managed and updated anti-virus program.

Anti-virus software must be active, scheduled to perform virus checks at regular intervals, and have its virus definition files kept up-to-date.

Any activities with the intention to create and/or distribute malicious programs onto the College network (e.g. viruses, worms, Trojan horses, email bombs, etc.) are strictly prohibited.

If an employee or student receives what they believe to be a virus or suspects that a computer is infected with a virus, it must be reported to the Information Technology department immediately by calling (563) 884-5300. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the Information Technology department.

Any virus-infected computer will be removed from the network until it is verified as virus-free.

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.

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 Policies, Processes And/Or Procedures

This Policy is supplemented below. It is the responsibility of all employees and students to know and comply with policies and procedures as supplemented.

Policies

- N/A

Processes And/Or Procedures

- N/A

Forms/Instructions

- N/A

Other Related Information

- Consumer Information

Contacts

Information Technology

Davenport, Ia. Campus

- Mark Wiseley
  Senior Director of Information Technology
  1000 Brady Street
  Davenport, IA 52803-5214
  (563) 884-5691
  mark.wiseley@palmer.edu

WEST CAMPUS, SAN JOSE, CALIF.

- Kelly Goetz
  Network Manager
  90 E. Tasman Drive
  San Jose, CA 95134-1617
  (408) 944-6104
  kelly.goetz@palmer.edu

FLORIDA CAMPUS, PORT ORANGE, FLA.

- Matt Kellen
  Network Manager
  4777 City Center Parkway
  Port Orange, FL 32129-4153
  (386) 763-2640
  matt.kellen@palmer.edu

Human Resources

- Senior Director for Human Resources
  Office of Human Resources
  1000 Brady Street
  Davenport, IA 52803-5214
  (563) 884-5866

HISTORY

Last Revised: ..... September 21, 2016

Revised: ..... February 2, 2010

Adopted: ..... N/A

Last Administrative Review: ..... September 21, 2016

Responsible Officer: ..... Aaron Christopher, Ph.D., CPA, CFE
Vice Chancellor for Administration
1000 Brady Street
Davenport, Iowa
(563) 884-5653
aaron.christopher@palmer.edu

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