Policy and Procedure:
COD Acceptable Use of Information Technology

<table>
<thead>
<tr>
<th>Responsible Office</th>
<th>Technology and Media Services</th>
<th>Effective Date</th>
<th>08/26/2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Official</td>
<td>Technology and Media Services Director</td>
<td>Last Revision</td>
<td>04/23/2017</td>
</tr>
<tr>
<td>Reviewed by</td>
<td>PHI Oversight and Review Committee</td>
<td>Review Date</td>
<td>04/21/2017</td>
</tr>
</tbody>
</table>

Scope
This policy applies to the College of Dentistry’s Acceptable Use of Information Technology

Policy
Technology, computers and the Internet play an important role in our daily work lives. Existing and changing technologies represent opportunities to enhance work processes, improve productivity and provide a better working and learning environment for our faculty, staff and students.

The use of computers and technology is extremely important to all collegiate faculty, staff and students and the use of collegiate resources should occur within the parameters of your specific responsibilities. Misuse of technology leads to lower productivity and increased support costs.

The University Operations Manual outlines your responsibilities using technology in the Acceptable Use of Information Technology Resources and the Ethics and Responsibilities for University Staff policies. Use the links below to familiarize yourself with these policies as they apply to all faculty, staff and students who use University or Collegiate IT resources. The last link is a list of all University IT policies.

http://cio.uiowa.edu/policy/AUP.shtml

http://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources

http://itsecurity.uiowa.edu/policy/

College of Dentistry policies do not replace, but rather complement University policies. In addition to the policies in the University Operations Manual, the College of Dentistry has the following policies and best practices.

- All computers and associated technology equipment should be used for collegiate business only.
- Personal USB devices, with the exception of encrypted flash drives, should never be plugged into a collegiate computer. This includes, but is not limited to, printers, keyboards, mice, etc.
- Personal files should not be stored on Dentistry file servers or computers. This includes personal photos, documents, spreadsheets, etc.
- Copyrighted material (music and movie files, games, and other personal software) should never be stored on Dentistry computers.
• Your University email account is considered University property and should be used accordingly.
• Internet access should be limited to web sites that help you do your job. University guidelines for accessing social media sites can be found at http://hr.uiowa.edu/policies/social-media-use-internet.
• Always exit MiPacs and axium, in that order, when leaving an operatory. Leaving patient data on the screen that others may see is a HIPAA violation.
• Never store PHI (Protected Health Information) on portable storage media such as flash drives, external hard drives or local computer hard drives. All PHI must be stored on network file space or the University’s approved cloud storage, OneDrive.

Your use of University computing resources is not completely private. While individual usage is not monitored, The University or College may inspect files or monitor usage when there is probable cause to believe a user has violated a University or Collegiate policy. In addition, users should be aware that their right to privacy in electronic records may be subject to the University’s obligation to respond to subpoenas or other court orders, reasonable discovery requests, and requests for documents pursuant to Iowa Code Chapter 22, the Public (Open) Records Law.

Patient medical and dental information retained by the College is protected by State and Federal laws which prohibit any disclosure without specific written consent of the person to whom it pertains, or as otherwise required by law. Patient healthcare data that is maintained electronically provides considerable access and management advantages. The potential for misuse of this confidential information has prompted significant governmental regulatory measures and standards legislation. In response, the College will be continually modifying its clinical and non-clinical security and privacy procedures in order to remain compliant. This currently includes random audits of appointments, providers and users who access patient information in our Clinical Information Systems.

By using collegiate information technology facilities and resources, users agree to abide by all related University and College procedures and policies, are subject to normal requirements of University and collegiate ethical behavior, as well as applicable federal, state, and local law. Violations may result in University and/or collegiate disciplinary action or referral to appropriate external authorities.

Resources