THE OHIO STATE UNIVERSITY
COLLEGE OF DENTISTRY

Information Systems Acceptable Use Policy

The information systems at The Ohio State University College of Dentistry are provided for the use of College students, faculty and staff, as approved, in support of the programs of the College. All students, faculty and staff are responsible for seeing that these information systems are used in an effective, efficient, ethical and lawful manner. The following policies relate to their use.

1. All computer and network systems that utilize University resources are also governed by the policies of the University (https://ocio.osu.edu/assets/Policies/Responsible-Use-of-University-Computing-and-Network-Resources-Policy.pdf), and users of those systems are required to adhere to those policies.

2. Unauthorized attempts to gain privileged access or access to any account or system not belonging to you on any College system are not permitted. All access to College information systems, including the issuing of accounts, must be approved through the department of Information Systems. All access to College and departmental information systems must be approved by authorized personnel.

3. Computer and network accounts provide access to personal, confidential data. Therefore, individual accounts cannot be transferred to or used by another individual. Sharing accounts or passwords is not permitted.

4. Computer and network accounts provide access to patient identifiable information, and as such, are covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which mandates requirements regarding privacy, security, and transmission of that information. No college user may access or store patient information on any system other than College approved and implemented patient management systems.

5. Each user is responsible for the proper use of his or her account and any activity conducted with it. This includes choosing safe, strong passwords, protecting them, and ensuring that file protections are set correctly. All users will be required to change their College network password at least once every sixty (60) days.

6. Each system user is responsible for the security of any system he/she connects to the network. A system seen to be attacking other systems, e.g. having fallen victim to viruses/worms, will be taken off the network, generally without notice, until it has been made secure.

7. No user shall connect any computer or device to the College network, in any manner, without first having the computer or device inspected and authorized by the Information Systems department.

8. No College system or network may be used as a vehicle to gain unauthorized access to other systems.

9. Any user who finds a possible security lapse on any University system or network must report it to the system administrators. To protect your files and the system, don't attempt to use a system under these conditions until the system administrator has investigated the problem.

10. All users should be aware that the system administrators conduct periodic security checks of College systems and networks, including password checks. Any user found to have an easily guessed password will be required to choose a secure password during his or her next login process.

11. User files on College systems are kept as private as possible. Attempts to read another person's protected files will be treated with the utmost seriousness. The system administrators will not override file protections unless necessary in the course of their duties, and will treat the contents of those files as private information at all times.

12. No College system or network may be used for any purpose or in a manner that violates University policies or regulations or federal, state or local law.

13. Please keep in mind that many people use College systems and networks for daily work. Obstructing this work by consuming gratuitously large amounts of system resources

14. Obstructing this work by consuming gratuitously large amounts of system resources (disk space, CPU time, print quotas, network bandwidth) or by deliberately crashing the machine(s) will not be tolerated.

15. Use of any College system by individuals or organizations not affiliated with the College requires special permission from the system's administrator and may require payment of fees to the University and to the appropriate software vendors where applicable.

16. Use of College systems or networks for commercial purposes, except where explicitly approved, is strictly prohibited. Such prohibited uses include, but are not limited to, development of programs, data processing or computations for commercial use and preparation and presentation of advertising material.

17. Frivolous, disruptive, or inconsiderate conduct in computer labs or terminal areas is not permitted.

18. No College computing facility may be used for playing computer games.

19. Copying, storing, displaying, or distributing copyrighted material using College systems or networks without the express permission of the copyright owner, except as otherwise allowed under the copyright law, is prohibited. Under the Federal Digital Millennium Copyright Act of 1998, repeat infringements of copyright by a user can result in termination of the user's access to College systems and networks.

20. No e-mail may be sent or forwarded through a College system or network for purposes that violate University statutes or regulations or for an illegal or criminal purpose.

21. Electronic mail, like user files, is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness. The College and its administrators of e-mail systems will not read mail unless necessary in the course of their duties. Also, there may be inadvertent inspection in the ordinary course of managing and maintaining the computer network and in carrying out other day-to-day activities.

22. Users should be aware that their "deletion" of electronic information will often not erase such information from the system's storage until it is overwritten with other data and it may, in any case, still reside in the College's network either on various back-up systems or other forms, and even if erased, may still exist in the form of print-outs.

23. Nuisance e-mail or other online messages such as chain letters, obscene, harassing, or other unwelcome messages are prohibited.

24. Unsolicited e-mail messages to multiple users are prohibited unless explicitly approved by the appropriate College authority.

25. All messages must show accurately from where and from whom the message originated, except in the rare, specific cases where anonymous messages are invited.

26. The College reserves the right to refuse mail and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses to University or other users, and to filter, refuse or discard such messages.

Violations of these policies may result in the immediate suspension of computer account and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations of the policy will be referred directly to the appropriate College or outside authorities; unauthorized use of College computing facilities can be a criminal offense. The penalties may be as severe as suspension or dismissal from the College and/or criminal prosecution.

The Ohio State University
College of Dentistry and Dental Faculty Practice
Information Systems Acceptable Use Policy Acknowledgement

Name: _____

Division (for Faculty, Staff, Visitors): _____

or

Class of (for Students): _____

University Email: _____

My signature below indicates that I have read, understand and agree to the Information Systems Acceptable Use Policy. I understand that a violation of any part of this policy could result in suspension of my access to computer resources at the College of Dentistry.

_____ _____

Signature Date

Please return this signed page to the Division arranging your visit.