Ochsner Clinical School

Policy

TITLE: Internet Access and Use

EFFECTIVE DATE: January 1, 2010; Revised April 1, 2021

APPROVER(S): Dean of Medical Education, OCS Head of School

NUMBER: OCS 15329-3

I. Purpose

***Ochsner Clinical School Students will adhere to all institution policies and guidelines for internet access and use. Institution Policy # 15329-3 follows. "Student" can be substituted for "employee" in the institutional policy.**

Use of the Internet by Ochsner Clinic Foundation (OCF) employees is subject to review, approval, audit and possible restriction as deemed necessary by OCF management. OCF may, at its discretion, monitor and record any and all Internet usage. No employee should have any expectation of privacy as to his or her Internet usage. Further, OCF reserves the right to inspect any and all files stored in private areas of our network as well as drives attached to any Ochsner-owned computer in order to assure compliance with this policy. At OCF, employees are expected to access the Internet primarily for business-related purposes, to conduct themselves honestly and appropriately while on the Internet, and to respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as in any other business dealings. All existing OCF policies apply to conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of OCF resources, sexual harassment, information and data security, and confidentially. Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity or expose OCF to significant legal liabilities. While OCF's direct connection to the Internet offers potential benefits, it also opens doors to significant risks to data and systems if employees do not follow appropriate security discipline. Security is to be everyone's concern. OCF employees will be held accountable for any breaches of security or confidentiality or for inappropriate use of OCF's Internet facilities.

II. Policy Statements

I. User ID's and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource from OCF, must keep that password confidential. OCF policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.

II. OCF has installed an Internet firewall to assure the safety and security of its network. Any employee who attempts to disable, defeat or circumvent any OCF security facility will be subject to immediate dismissal.

III. Only those Internet services and functions with documented business purposes for OCF will be enabled at the Internet firewall.

IV. Any file that is downloaded from the internet will be scanned for viruses before it is sent to the intended recipient. Suspected viruses should be reported to the IS Customer Service Center.

V. Files containing confidential OCF data and in particular patient specific data that are transferred in any way across the Internet must be appropriately encrypted. Questions regarding confidentially and encryption should be referred to the IS Division.

VI. Employees should schedule communication-intensive operations such as large file transfers, video downloads, mass e-mailings and the like for off-peak times. Such activities that degrade Ochsner network services will be terminated.

VII. The display of any kind of sexually explicit image or document on any OCF system is a violation of our policy on sexual harassment. Since a wide variety of materials may be considered offensive by colleagues, customers or suppliers, it is a violation of OCF policy to store, view, print or redistributes any document or graphic file that is not directly related to the user's job or OCF business activities.

VIII. OCF may use independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to any such sites. Any Ochsner employee connected incidentally to a site that contains sexually explicit or offensive material must disconnect from that site immediately.

IX. Employees with Internet access may not use OCF Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.

X. Employees with Internet access may not use OCF Internet facilities to download videos unless there is an express business-related use for the material.

XI. In the event of suspected unauthorized or inappropriate Internet use, employees should inform their department manager who may request assistance from IS management. IS management will notify the appropriate IS employees who will respond immediately to the reporting department by beginning a security incident report and investigation. All parties involved shall treat all information and aspects of the investigation with the highest level of confidentiality.

XII. OCF's Internet facilities and computing resources must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other local jurisdiction in any material way.

XIII. Any software or files downloaded via the Internet into the Ochsner network become the property of OCF. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

XIV. Employees with Internet access may download only software with direct business use and must arrange to have such software properly licensed and

registered. Downloaded software must be used only under the terms of its license.

XV. No employee may use OCF facilities to download or distribute pirated software or data.

XVI. Employees with Internet access may not upload any software licensed to OCF or data owned or licensed by OCF without the express authorization of the manager responsible for the software or data.

XVII. No employee may use OCF Internet facilities to propagate any virus, worm, Trojan horse, trap door, or similarly harmful program code.

XVIII. No employee may use OCF Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

XIX. In the interest of keeping employees well informed, use of news briefing services like Pointcast is acceptable, within limits that may be set by each department's managers.

III. Enforcement

Failure to comply with this policy may result in progressive discipline up to and including termination of employment for employees or termination of contract or service for third-party personnel, students or volunteers.