# Internet Usage Policies
# Green Street Dental Group ®

Company-supplied technology, including computer systems, belong to Green Street Dental Group, not the employee.

1. Green Street Dental Group has software and systems in place that can monitor and record all Internet usage. We want you to be aware that our security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. We may review Internet activity and analyze usage patterns, and may choose to publicize this data to assure that company Internet resources are devoted to maintaining the highest levels of productivity.

2. Access to the internet is provided to staff as a business tool to assist in the day-to-day performance of workplace duties.

3. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

4. The display of any kind of sexually explicit image or document on any company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

5. The company uses independently-supplied software and data to identify inappropriate or sexually-explicit Internet sites. We may block access from within our networks to all such sites that we know of. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

6. This company's Internet facilities and computing resources must not be used knowingly 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. Use of any company resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.

7. Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights, and must be approved for download by management, which at time of this transcript and for this purpose, consists of Dr. Jablow only. 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.

8. No employee may use company facilities knowingly to download or distribute pirated software or data.

9. No employee may use the company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

10. No employee may use the company's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

11. Each employee using the Internet facilities of the company shall identify himself or herself honestly, accurately and completely (including one's company affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

12. Employees may use their Internet facilities for non-business research or browsing during meal time or other breaks, or outside of work hours, provided that all other usage policies are adhered to.

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

14. The company has installed a variety of firewalls, proxies, Internet address screening programs and other security systems to assure the safety and security of the company's networks. Any employee who attempts to disable, defeat or circumvent any company security facility will be subject to immediate dismissal.

15. No employee will open (click on) any e-mail attachment unless approved by management, with the exception of .jpg files.

"I have a received a written copy of my company's Internet usage policy. I fully understand the terms of this policy and agree to abide by them. I realize that the company's security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to dismissal or even criminal prosecution."

_____

Employee Signature Date