



RCI COMPUTER AND TELECOMMUNICATIONS USE POLICY

The purpose of this policy is to regulate the proper use of the computers, software and telecommunications system of Radiology Consultants of Iowa, PLC (Employer).

- **Ownership of Facilities.** The computers, software and telecommunications system (“Facilities”) belong to the Employer. Employees are given access to the Internet and to the Facilities to help them perform their job duties and further Employer’s interests.
- **Proprietary Information.** Radiology Consultants of Iowa proprietary information stored on electronic and computing devices whether owned or leased by Radiology Consultants of Iowa, the employee or a third party, remains the sole property of Radiology Consultants of Iowa. You have a responsibility to promptly report the theft, loss, or unauthorized access or disclosure of proprietary information.
- **Use of Facilities.** Except for limited occasional personal use, the Facilities are to be used for authorized business purposes only. Employer will determine in its sole discretion the scope of permissible occasional personal use.
- **Use of Equipment.** Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.
- **Access.** Employees may access the Internet only through the network using Employer’s Internet connection.
- **Security Concerns.** Employees are encouraged to report any suspicious behavior, including suspicious links and attachments, to security or IT personnel. False alarms are not subject to disciplinary action.
- **Prohibited Use.** Employees may not use the Facilities for commercial advertisements, solicitations, or promotions other than on behalf of the Employer and to further the Employer’s interests; for personal advertisements, solicitations, or promotions; for the dissemination of destructive programs such as virus software and self-replicating code; for the dissemination of political material; or for any other unauthorized use.
- **Prohibited Activities.** Use of the Facilities to further any unlawful purpose is prohibited. Transmitting, receiving, displaying, printing, forwarding, or otherwise disseminating material that is fraudulent, illegal, harassing, offensive, embarrassing, sexually explicit, obscene, threatening, or defamatory is prohibited.

- **Social Media and Blogging.** Employees shall not engage in any blogging or dissemination of other social media that may harm or tarnish the image, reputation and/or goodwill of Radiology Consultants of Iowa and/or any of its employees. Employees are also prohibited from making any political, discriminatory, disparaging, defamatory or harassing comments when blogging or posting on social media.
- **Social Media and Blogging.** Employees may also not attribute personal statements, opinions or beliefs to Radiology Consultants of Iowa when engaged in blogging or posting on social media. If an employee is expressing his or her beliefs and/or opinions in blogs or social media posts, the employee may not, expressly, or implicitly, represent themselves as an employee or representative, or otherwise associated with Radiology Consultants of Iowa. Employees assume all risk associated with blogging.
- **Codes.** Access codes must be disclosed to the Employer. The use of unauthorized codes or passwords to gain access to files on the Facilities is prohibited.
- **Trade secrets disclosure.** Employer's trade secrets/confidentiality policy applies to the Internet and the Facilities. In communicating with others, exercise at least the same level of care in what you reveal as you do when using other forms of communication. The Internet is not a secure medium unless encryption or other similar measures are taken. Sensitive or confidential information should not be communicated over the Internet unless security safeguards are in place.
- **Commitments on Behalf of Employer.** Statements made in emails may be misinterpreted or otherwise may operate to obligate the Employer in some manner. Employees should use the same level of care in email messages that they use in other forms of communication. In particular, Employees should not make negative statements about the products, competence, professionalism, and/or advertising/statements of third parties.
- **Viruses.** All material downloaded from the Internet or from computers or networks that do not belong to the Employer must be scanned for viruses before being placed onto the Facilities.
- **Password Composition.** Employees must use a 16-character password for their primary company network account in accordance with the company's password policy. The password must not be used for any other accounts or purpose. Employees with network administrator accounts must use a unique 20-character password to that account. Passwords are not to be revealed to anyone else including coworkers and family members.
- **Waiver of Privacy.** Employer has the right but not the duty to monitor any and all aspects of its computer system, including, but not limited to, reviewing email sent and received by employees; monitoring chat rooms and newsgroups; reviewing material downloaded or uploaded by employees; and monitoring Web sites visited by employees. By signing this policy, Employee understands and acknowledges that he/she has no right

of privacy related in any way to the use of Employer's computer system and, further acknowledges that email messages sent or received using the Facilities are business messages which belong to the Employer, and not personal, confidential information belonging to the Employee.

- **Intellectual Property Laws.** Employees using the Facilities must respect and avoid infringing the intellectual property rights of others, including but not limited to copyrights, trademark rights, patent right, trade secret rights, and publicity and privacy rights. Copying material from Web sites without permission may be copyright infringement. Use of the Facilities to violate third-party intellectual property rights is strictly prohibited.
- **Sexual Harassment and Non-Discrimination Policy.** Employer's policy prohibiting sexual harassment and discrimination applies to the Internet and Facilities.
- **Medical Records.** Employer's computer system may allow an employee access to medical records of the patients of Radiology Consultants of Iowa, PLC. Such medical records are confidential and are not to be accessed by any employee unless for a clearly legitimate business-related reason.
- **Personal Accounts/Personal Use.** An employee should not access his or her personal accounts using Employer's computer system. Each employee is solely responsible and shall be personally liable (legally, financially, or otherwise) for the employee's use of Employer's computer systems outside the scope of the employee's employment.

I have read this Policy and agree to comply with it. I understand that violation of this Policy may result in disciplinary action, including possible termination and legal action.

Signed:

Printed Name:

Date: