|  |  |
| --- | --- |
| **Policy #:HRM.01.01.03** | **Effective Date:**  07/02/15 |
| **JCAHO Section:**  Human Resources | **Revised Date**:  01/01/ 2019 |
| **Applicable Program/Department:**  Outpatient Clinical Services | **Members of Committee**:  Janet Ward, Pres/CEO, Wilda Davis, Clinical Supervisor, Jennifer Wilson, HRM |
| **Executive Staff Approval:**  **Signature**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Title:** President/CEO Mrs. Janet Ward  **Date:** | **Board Approval**  **Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Title:** Chairperson - Sony Fenelon  **Date:** |

**SCOPE:**

The policy applies to all employees of Parent’s Information & Resource

**RESPONSIBILITY:**

It is the responsibility of the Director and/or designee to implement this policy and procedure. It is the responsibility of the Director and Supervisor of each site and or program to disseminate this information to employees under their supervision.

Voice mail, email, and Internet usage assigned to an employee's computer or phone extensions are solely for the purpose of conducting Company business. Some job responsibilities at the Company require access to the Internet and the use of software in addition to the Microsoft Office suite of products. Only people appropriately authorized, for Company purposes, may use the Internet to access additional software.

**Software Access Procedure**

Software needed, in addition to the Microsoft Office suite of products, must be authorized by your supervisor and downloaded by the IT department. If you need access to software or websites, not currently on the Company network, talk with your supervisor and consult with the IT department.

**Company Owned Equipment**

Any device or computer including, but not limited to, desk phones, cell phones, tablets, laptops, desktop computers, and iPads that the Company provides for your use, should only be used for Company business. Keep in mind that the Company owns the devices and the information in these devices. If you leave the Company for any reason, the Company will require that you return the equipment on your last day of work.

**Internet Usage**

Internet use, on Company time, is authorized to conduct Company business only. Internet use brings the possibility of breaches to the security of confidential Company information. Internet use also creates the possibility of contamination to our system via viruses or spyware.

Spyware allows unauthorized people, outside the Company, potential access to Company passwords and other confidential information.

Removing such programs from the Company network requires IT staff to invest time and attention that is better devoted to progress. For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit Internet use.

Additionally, under no circumstances may Company owned computers or other electronic equipment, including devices owned by the employee, be used on Company time, to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related Internet sites. Personnel telephone usage is prohibit. Doing so can lead to disciplinary action up to and including [termination of employment](file:///C:\od\glossaryt\g\termination.htm).

**Social Media**

Your employer understands that part of what you do in [social media](file:///C:\od\glossarys\g\social-media.htm) is outreach that recruits new employees and enhances our Company brand. Many employees have social media responsibilities in their job description including the social media marketers, tech support, and recruiters.

Your employer also understands that the relationship of our employees to an online world that you spend time in 24/7 can lead to the blurring of work time and off work time. We strongly encourage you to limit the use of social media to work-related content and outreach during work hours.

Additionally, you are prohibited from sharing any confidential or protected information that belongs to or is about the Company. You are strongly encouraged not to share disparaging information that places your Company or coworkers in an unfavorable light. The Company's reputation and brand should be protected by all employees. The lives and actions of your coworkers should never be shared online.

In social media participation from work devices or during working hours, social media content that discriminates against any protected classification including age, race, color, religion, sex, national origin, disability, or genetic information is prohibited. It is our company policy to also recognize sexual preference and weight as qualifying for discrimination protection. Any employee, who participates in social media, who violates this policy will be dealt with according to the [harassment](file:///C:\od\discrimination\a\what-is-harassment.htm) policy.

**Email Usage at Company**

Email is also to be used for Company business only. Company confidential information must not be shared outside of the Company, without authorization, at any time. You are also not to conduct personal business using the Company computer or email.

Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste company time and attention.

Viewing pornography, or sending pornographic jokes or stories via email, is considered [sexual harassment](file:///C:\od\glossarys\a\sexualharassdef.htm) and will be addressed according to our sexual harassment policy.

**Emails That Discriminate**

Any email content that discriminates against any protected classification including age, race, color, religion, sex, national origin, disability, or genetic information is prohibited. It is our company policy to also recognize sexual preference and weight as qualifying for discrimination protection. Any employee who sends email that violates this policy will be dealt with according to the [harassment](file:///C:\od\discrimination\a\what-is-harassment.htm) policy.

These emails are prohibited at the Company. Sending or forwarding non-business emails will result in disciplinary action that may lead to [employment termination](file:///C:\od\glossaryt\g\termination.htm).

**Company Owns Employee Email**

Keep in mind that the Company owns any communication sent via email or that is stored on company equipment. Management and other authorized staff have the right to access any material in your email or on your computer at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored on work systems.

**Telephones:**

In order to maintain a productive and client-focused environment, employees are requested to restrict the personal use of the telephone, for both incoming and outgoing calls, to emergency situations only.

**Electronic Media/Computer Usage:**

Most employees have access to computer, e-mail, telephones, voice mail, and fax machines and in some cases online services. PIRC maintains the right to monitor and review all information created and/or communicated by an employee via electronic media. Electronic media may not be used for discriminatory, harassing or obscene communications, personal gain, advancement of individual opinions, or for any other purpose, which is illegal, or against company policy or PIRC. Employees may not use a code, access a file, retrieve stored information or disseminate information, unless authorized to do so. An employee’s occasional use of PIRC computer facilities to type a term paper for an educational course or prepare announcements for a charitable event is acceptable. However, in order to keep these uses to a reasonable level, approval to use the system in such a manner must be given by the employee’s supervisor. Moreover, please be aware that files may be purged at any time, without notice. The use of the system for such personal efforts must occur outside of business hours and any files created are to be deleted at the end of the project.

To preserve the integrity of the computer network from viruses, all software downloads must be handled through the MIS Department or Systems administrator. Any employee abusing the privilege of company- facilitated access to electronic media may be subject to disciplinary action, up to and including discharge.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_

Staff Signature & Credentials Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_

Personnel Representative Date