EMPLOYEE COMMUNICATIONS

Bulletin Boards

Each building has a bulletin board, which is used to communicate important agency information. All posted items must be approved in advance by the Executive Director, and/or a designee appointed by the Executive Director.

The employee is responsible for regularly reading the information posted on the bulletin boards.

Agency Communications Systems Security Policy

All materials, messages and information created, transmitted or stored via computer, electronic mail, or voice mail are the property of the agency and may be accessed by authorized personnel. JLR&CS reserves the right to monitor these systems. Users should have no expectation of privacy with respect to materials and information created or transmitted or stored on these systems. Use of computers or the voice mail and e-mail systems by an employee grants consent to management to monitor any usage or mail messages.

JLR&CS is committed to protecting its employees, clients, partners, affiliates, and the agency from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of JLR&CS. These systems are to be used for business purposes in serving the interests of the agency and the individuals served.

Effective security is a team effort involving the participation and support of every JLR&CS employee accessing the computer system and affiliates who deal with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment at JLR&CS. These rules are in place to protect the employee and JLR&CS. Inappropriate use exposes JLR&CS to risks including virus attacks, compromise of network systems and services, and legal issues. This policy applies to employees, contractors, consultants, temporaries, and other workers at JLR&CS, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by JLR&CS.

General Use and Ownership

1. JLR&CS' users should be aware that the data they create on the corporate systems remains the property of JLR&CS. Because of the need to protect JLR&CS' network, management does not guarantee the confidentiality of information stored on any network device belonging to JLR&CS.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

3. For security and network maintenance purposes, authorized individuals within JLR&CS may monitor equipment, systems and network traffic at any time.
4. JLR&CS reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: corporate strategies, proprietary information, competitor sensitive information, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. All PCs, laptops and workstations should be secured by logging-off when the computer will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by employees from a JLR&CS email address to newsgroups is not allowed unless posting is in the course of business duties.
6. All computers used by the employee that are connected to the JLR&CS Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code and thus, infect the network. Employees must contact Information Technology immediately if they have any questions or concerns regarding an email.

Unacceptable Use

This section includes activities that, in general, are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a computer user if that user is disrupting production services).

Under no circumstances is an employee of JLR&CS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing JLR&CS owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by JLR&CS.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which JLR&CS or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing employee account passwords to others or allowing use of the employee's account by others. This includes family and other household members if work is being done at home.
6. Using a JLR&CS computing asset to actively engage in procuring or transmitting material that is in violation of harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any JLR&CS account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless a prior notification to JLR&CS is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, JLR&CS employees or clients to parties outside JLR&CS.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within JLR&CS' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by JLR&CS or connected via JLR&CS' network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

Personal Websites and Social Networking Policy

JLR&CS respects the right of employees to use and develop personal websites and web logs (blogs) during their personal time and to participate in social networking services, chat rooms, bulletin board posting, and other web facilities. The employee must adhere to the following guidelines:

- Make it clear that the views expressed are the employee's alone and that they do not necessarily reflect the views of JLR&CS;
- Do not disclose any information that is confidential or proprietary, or any intellectual property, trademark or logo of JLR&CS;
- Avoid making defamatory statements about JLR&CS, its employees, clients, partners, affiliates and others, including competitors. Otherwise the employee may be subject to legal liability; and
- Blogging must never interfere with the employee's job.

If blogging activity is perceived to conflict with an employee's employment, the agency may ask the employee to discontinue the activity, and the employee may be subject to disciplinary action. For any questions about these guidelines, contact the Associate Director.

Audio/Videotaping Prohibited

Employees may not audiotape or videotape, or assist in taping, any other employees, operations or clients of the agency without written consent of management and all participants.

INFORMATION SECURITY AGREEMENT

Acknowledgement

I acknowledge that I have received and read the JLR&CS Agency Communications Systems Security Policy included in the Employee Handbook. I understand that I must comply with it when accessing and using information resources. My failure to comply with the Security Policy may result in cancellation of my privilege of use, appropriate disciplinary action (up to and including termination), and action by law enforcement authorities.

By signing this Information Security Agreement, I also indicate my understanding of my personal responsibilities in maintaining JLR&CS clients' rights to privacy. I agree that I will only access information of the clients for whom I am directly providing or supporting clinical care.

_____ _____

Signature/Date **Printed Name (Last, First, Middle Initial)**