INFORMATION TECHNOLOGY

POLICY ELECTRONIC COMMUNICATIONS & ACCEPTABLE USE OF TECHNOLOGY

I. POLICY

The purpose of this Policy is to outline the acceptable uses of technology at CB Richard Ellis (ìCBRE î or the ìCompanyî) in order to protect the substantial investment that the Company has made in its various technology and electronic communications systems, including but not limited to its telephone, voicemail, fax and e-mail systems; computers, including fileservers and Web servers; software, including operating systems, applications, platforms and fonts; storage media; network accounts; Internet access/browsing; instant messaging; file transfer protocols (FTP); PDAís, and Blackberries, cell phones and similar devices (collectively ìelectronic communication systemsî). The Companyís electronic communication systems are tools for business communication, and all employees have the responsibility to use these resources in an efficient, effective, ethical and lawful manner, consistent with this Policy, for the benefit of the Company.

This Policy applies to everyone using any equipment (e.g., CBRE, personal, client) to access the electronic communication systems, including but not limited to independent contractors or employees working remotely.

Failure to abide by this Policy, including failure to consent to any interception, monitoring, copying, reviewing or downloading of any communications or files, is grounds for disciplinary action, up to and including termination of employment and may subject the violator to legal action.

II. PROVISIONS AND CONDITIONS

A. General

1. The electronic communication systems and all information transmitted by, received from or stored in these systems are the sole property of CBRE. Even though users maintain personal passwords, they should have no expectation of privacy in connection with the use of any systems or regarding any information created, stored or transmitted by them. The ìdeletionî of a message or file may not eliminate the information from these systems and users should have no expectation of privacy for deleted information.

2. Consent and compliance with this policy is a term and condition of employment. To ensure that the use of electronic communications and computer systems is consistent with the Company's legitimate business interests or to evaluate employee performance or compliance with policy or law, authorized Company representatives (including, at times, third parties retained by the Company) may monitor the use of these systems and equipment from time to time, which may include printing and reading information entering, leaving or stored in these systems. Anyone using any system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of illegal activity, the Company may provide the evidence to law enforcement officials.

3. The electronic communication systems are intended to be used for business purposes. Incidental and occasional personal use of these systems is permitted, so long as it does not interfere with the performance of the systems and does not otherwise violate this Policy. Personal information stored in the electronic communication systems is subject to the same monitoring activities as business-related information. These systems must not be used to conduct business activities outside Company business, including solicitations for political, charitable, personal or other causes. If you have any question about the reasonableness of any personal use of these systems, check with your manager.

4. Use of the electronic communication systems will be governed by the same standard as all other business activities. All Company policies and practices, including those concerning harassment, discrimination and solicitation, apply fully to these systems and their users.

5. Employees are expected to use good judgment in the use of the Company's systems and should exercise the same restraint and caution in creating electronic messages that they would use in writing formal paper documents. Specifically, employees should address messages to recipients who need to know the information and use prudence when sending attachments. Employees should construct messages professionally (spelling, grammar) and efficiently (subject, field, attachments), with the same standards expected in written business communications and public meetings. Confidential messages should include a warning regarding accidental transmission to an unintended third party, which should be a part of the standard email signature block.

6. Users are required to follow the CBRE password policy and select a confidential, non-trivial password for use with their system account(s). Users are responsible for all actions associated with their account and password. Accordingly, no one should share their account and passwords with others and everyone must change their password on a regular basis to avoid unauthorized access. The same protocols should be followed for passwords selected by users for the voicemail system and any other electronic system requiring a password.

7. All computers used by employees that are connected to the electronic communication systems, whether owned by the employee, a third party, or CBRE, should continually be executing approved virus-scanning software with a current virus definition, current critical security patches, and firewall protection. Users are expected to be responsible for maintaining their systems such that they are free of any software that could cause damage (e.g., key logger, worm, virus) to CBRE electronic communication systems. In addition, users should utilize the lockout feature on all PCs, laptops and workstations when they are not attended.

B. Unacceptable Uses

Material, data or other information, including but not limited to material determined by the Company in its sole discretion to be offensive, harassing, obscene, pornographic, threatening, discriminatory or defamatory or which otherwise violate any state, local or federal law or Company Policy (hereby referred to as ìInappropriate Materialî) is prohibited on the electronic communications systems.

The activities described below would be considered a violation of this Policy and may result in discipline. Failure to abide by these rules and guidelines, including failure to consent to any interception, monitoring, copying, reviewing or downloading of any communications or files, is grounds for discipline, including monetary fines, reprimands

and/or termination of employment. This list is by no means exhaustive, but instead is an attempt to provide a framework to judge activities that are unacceptable.

1. The creation and exchange (even between willing participants) of messages or attachments containing Inappropriate Material.

2. The distribution of Inappropriate Material to employees, clients, vendors or customers outside of the Company ñ whether the distribution was intended or inadvertent. (This violation will result in the most severe penalties, and may include termination of employment, even on the first offense. A second offense will likely result in the termination of employment.)

3. Sending unsolicited messages or communications, including junk mail, jokes, chain letters or advertising material to individuals who did not specifically request such material (e-mail spam). This provision includes business-related email advertisements, such as property marketing and other business promotion materials. All advertising material must comply with the provisions of the CAN-SPAM Act, including required disclosures and opt-out procedures. To ensure compliance and protect employees and the Company, all email advertising must be created, sent and managed though the Companyís approved email marketing campaign system. Failure to comply puts the Company at risk and cannot be tolerated.

4. The intentional creation or dissemination of computer viruses, or any unauthorized, deliberate action which damages or disrupts the Company's electronic communication systems, alters their normal performance, attempts to circumvent or disable system monitoring and controls, or causes them to malfunction. (In addition, users should not open attachments to e-mails or other communications such as instant messages received from unknown senders since the attachments may contain viruses or unknown software.)

5. Inappropriate or excessive use of the Internet for non-business purposes. This includes, but is not limited to, the viewing of websites or connecting to Internet services with Inappropriate Material, and will be enforced by the Company through web filtering, among other technological means.

6. Introduction of unauthorized software (i.e., screensavers, toolbars, music players, etc.) on computers or the electronic communications system. IT must authorize all software deployed on CBRE devices.

7. Use of the electronic communication systems to attempt to gain unauthorized access to any remote system, including by circumventing user authentication or security of any computer, network or account.

8. Unless explicitly authorized by IT in writing, establishing Internet or other external network connections (such as hosts with public modem dial-ins, wireless, websites and FTP) that could allow unauthorized persons to gain access to the electronic communication systems and information stored therein.

9. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Exceptions: An account and password may be provided to IT support employees, such as the Help Desk to assist in troubleshooting, or for special IT projects. IT will always advise users to reset passwords after issue is resolved.

10. The unauthorized exchange or disclosure of or access to proprietary or confidential information, trade secrets or any other privileged, confidential or sensitive information relating to CBRE, a client or the business of either via any method of communication, including the electronic communication systems. This includes employees who use 3rd party services to communicate confidential information (e.g. message boards, websites and blogs).

11. Providing proprietary information about, or lists of, CBRE employees, customers, e-mail addresses, vendors, or product information to parties outside of CBRE without proper authorization.

12. The creation and exchange of advertisements, solicitations, sale of tickets or personal property, or chain letters.

13. The creation, copying and/or exchange of information (including copyrighted images, software, fonts or music) in violation of any copyright laws and the installation of any copyrighted software, including fonts for which CBRE does not have an active license.

14. Registration to list servers or subscribing to email lists without proper authorization. (Subscription to such a service can result in an overload of received messages directly impacting the performance of the e-mail system.)

15. Reading or sending messages from another userís account except under proper delegation arrangements, or unauthorized use of or altering of e-mail address information.

16. Accessing a file or retrieving any stored information or data from a file other than those for which access has been authorized (and then only for the purpose of conducting Company business).

17. Sending unsolicited faxes. See Policy ìRestrictions on Marketing by Faxî for additional information.

18. Making sales calls to residential phone numbers listed on the ìDo Not Call Registryî unless they are a recent customer (within the past 18 months) or have given permission in writing.

19. CBRE values open and direct communication between employees, clients, and the company. Accordingly, you may not make an audio or videotape or digital recording of any conversations, meetings, events, or other activities by or between CBRE employees or clients without the consent of all the individuals involved. Consent may be given in writing before the recording or by confirmation of the consent on the recording itself.

    CBRE may record meetings, training sessions, and other company-sponsored events or meetings for company purposes. CBRE may also record activities, conversations or meetings on its premises for security purposes or in conjunction with or part of a company investigation of misconduct. CBRE may also conduct searches of company property, such as a work station, without advance notice or consent."

C. Response and Escalation

Employees who become aware of violations of this Policy should immediately report the violation to their immediate supervisor or manager or their local human resources representative, who should report it immediately to the Information Technology Security Officer.
If a user receives an e-mail or attachment containing Inappropriate Material or knows of such e-mails or attachments being sent by other employees, the following should be done:

1. If the e-mail is sent by an employee of the Company, you must report the matter to your manager, human resources, and/or any other manager immediately. Do not remove this e-mail until instructed to do so by a manager. The Company will take the necessary steps to remove and save the inappropriate e-mail.

2. If the e-mail is sent by someone not employed by the Company ñ whether from someone you know or not ñ please follow the following guidelines:

    a. If you know the sender, send it back to the sender and tell them not to send these types of e-mails to you at work again. If you want to receive the e-mails, ask that they be sent to your home personal computer, via your personal e-mail account. Continued receipt of such e-mails at work places you at risk of the disciplinary actions outlined above.

    b. Immediately delete the e-mail from your in-box, and then delete it from your ìdeleted itemsî folder to remove it from your system.

3. If there are any attachments to the e-mail, do not open them. If you open an attachment, a temporary copy may end up in your computer, which could inadvertently be discovered by someone else, which would lead to the disciplinary actions outlined above.

4. If you have inappropriate e-mails on your system now, you are required to remove them immediately and should follow the instructions in paragraphs 1 and 2 above, depending on whether the sender is a Company employee. If you need assistance in removing offensive e-mails or attachments, please contact your manager. No disciplinary action will be taken if you initiate the process of seeking assistance in removing this material from your computer.