606 - Can We Control Blogging, IM, & Other Employee Communication Inside the Workplace & Beyond?

Julienne Bramesco
Vice President & General Counsel
Colonial Parking

Robin McCune
Associate General Counsel
Strayer Education Inc.

Lynn Outwater
Regional Managing Partner
Jackson Lewis LLP

Technology and Communication

- Technology has created nearly limitless opportunities for employees to communicate
  - At work
  - About work

How Big is this Problem?

- 2006 Workplace E-mail, Instant Messaging, and Blog Survey
  - Conducted by the American Management Association and the ePolicy Institute
  - Based on responses from 416 companies
  - Results
    - 76% of employers have a policy governing employees' use of email at work
    - 31% of employers have a policy governing employees' use of instant messaging at work
    - 9% of employers have a policy governing employees' operation of personal blogs at work

How Big is this Problem?

- 2006 Workplace E-mail, Instant Messaging, and Blog Survey
  - E-mail
    - 31% of those surveyed by the AMA report spending more than 2 hours at work on email.
    - 42% of employers train workers about e-mail risks, policy, and usage
    - 34% of employers have e-mail retention and deletion policies
  - The Toll
    - 24% of employers have had employee e-mail subpoenaed
    - 15% of employers have gone to court to battle lawsuits triggered by employee e-mail
    - 26% of employers have fired employees for misusing e-mail at work

How Big is this Problem?

- 2006 Workplace E-mail, Instant Messaging, and Blog Survey
  - Blogs
    - 30% of the internet population visited blogs in the first quarter of 2005.
    - 8% of employers operate a business blog
    - 17% of employers block access to external blog web sites
    - 7% of employers have a policy governing what employees may put on their personal blogs at home
    - 2% of employers have had to discharge employees for inappropriate content in blogs

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success October 29-31, Hyatt Regency Chicago

How Big is this Problem?

- 2006 Workplace E-mail, Instant Messaging, and Blog Survey
  - Instant Messaging
    - 35% of employees use instant messaging at work
      - 26% of messages include non-work related attachments
      - 24% of messages include jokes, gossip, rumors, or disparaging remarks
      - 12% of messages include confidential company, employee, client information
      - 10% of messages include sexual, romantic, and pornographic chat
    - 2% of employers have fired workers for inappropriate instant messages

How Big is this Problem, cont'd.

- Internet use costs American businesses more than $178 million in lost productivity
  - Americans spent $608 million online on the Monday following Thanksgiving creating a new expression

    "Cyber Monday"

How Big is this Problem, cont'd.

- 60% of U.S. organizations engage in some form of email monitoring, but approximately the same number rarely or never track IM usage.
- Lawsuits
  - 26% of companies have terminated employees due to email conduct
  - 13% have been party to a lawsuit arising from email use
  - 20% have been ordered by a court to produce email.

Definitions

- Blog
- Dooce
- IM

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Case Study

- A male employee ("John") was uncomfortable with the attention he felt he received from an openly gay colleague ("Mike").
- These attentions allegedly were that Mike would stare at John and that he stole an "overt, purposeful, and glaring look" at John when both were in the restroom at the same time.

Case Study

- Instead of reporting the alleged harassment to his employer, John sent what he believed was an anonymous IM to Mike's computer that read, "Stop Staring! The Guys on the floor don't like it."
- Mike, believed that message was anti-gay harassment because of its anonymous nature and because he is openly gay.
- Mike reported his concern to Human Resources, claiming that he has a "lazy eye," which makes it appear that he may be staring even when he may not be.

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Case Study

- HR has come to you for assistance.
  - What do you advise them?
  - What, if any, disciplinary actions should management take?

Laws Impacting Employee Communication

- Harassment & Discrimination (Title VII of the Civil Rights Act of 1964, as amended, Americans with Disabilities Act, similar state statutes)
  - Communications between employees are often the basis for discrimination claims
  - Stored communications can be evidence of discrimination and/or harassment.

Harassment

- Laws require that an employer undertake reasonable efforts to prevent
- Duty to monitor generally begins with the employer's discovery
- Unless employer should have known before that

Negligent Hiring and Retention

- An employer may be liable for the wrongful acts of its employees if it knew or had reason to know of the risks the employment created

Business Proprietary Information

- Intellectual Property Infringement
  - IP Waivers
- Securities Law
  - Fair Disclosure Regulations
  - Insider trading
  - Fraud

Wiretap Act and Email Monitoring

- Electronic Communications Privacy Act of 1986
  - 18 USC §2510 et seq.
- Electronic communications covered

Defamation

- A false statement
- An unprivileged publication
- Fault amounting at least to negligence
- Special harm, if required

Privacy Rights

- Intrusion Upon Seclusion
- Publication of Private Facts
- False Light

Lawful Off-duty Conduct Statutes

- Arizona
- California
- Colorado
- Connecticut
- D.C.
- Illinois
- Indiana
- Kentucky
- Louisiana
- Maine
- Minnesota
- Mississippi
- Missouri
- Montana
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Oklahoma
- Oregon
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Virginia
- West Virginia
- Wisconsin
- Wyoming

The National Labor Relations Act, 29 U.S.C. Sec. Sec. 151-169

- applies to all employers regardless of whether or not the workforce is organized

Concerted Activity

- Non-union employees have protection of the Act when they engage in protected concerted activities.
  - Esco Elevators, 276 NLRB 1245, 120 LRRM 1214 (1985).
  - Meyers Industries, 281 NLRB 882, 123 LRRM 1137 (1986).

Other Implications of the NLRA

- March 2007 oral argument on email use
  - *The Register – Guard*, 2002 NLRB LEXIS 70 (NLRB Feb. 21, 2002).
- Confidentiality
  - *Cintas Corp. v. NLRB,* No. 05-1305 (D.C. Cir. Mar. 16, 2007).
- Anti-fraternization
  - *Guardsmark, LLC v. National Labor Relations Board*, 2007 U.S. App. LEXIS 2263 (D.C. Cir. Feb. 2, 2007).

Employee Privacy

- What is an employee's reasonable expectation of privacy at work
- O'Connor v. Ortega, 480 U.S. 760 (1987)

Other Reputation Issues

- Disclosure of private facts can damage a company's reputation
- Reputation harm is often a motivator in a union's corporate campaign
- Loyalty obligations of employees

E Discovery

- Rule 26 Amendments Federal Rules of Civil Procedure
- Develop your Safe Harbor
- Involvement of IT department

Best Practices

- Communicate and maintain an up-to-date electronic communications policy
- Train your employees, contractors, and anyone who uses your IT systems
- Have IT designate a point person
- Confer with IT immediately upon receiving litigation to commence litigation holds

Best Practices Cont'd

- Know state laws governing privacy and lawful off-duty activity
- Manage electronic communication monitoring
- If you do allow personal use of company systems, don't ignore the productivity implications
- Keep company communications on company systems

Best Practices Cont'd

- Conduct annual ethics and confidentiality training
- Review policies and update regularly
- Beware of creating zones of privacy
- Negotiate any changes of working conditions with the appropriate unions

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success October 29-31, Hyatt Regency Chicago

Insights Labor & Employment

Challenges in cyberspace

How to protect your company against the threat of employee blogging **Interviewed by Lindsey Grant**

Workplace blogs are growing in popularity and creating problems for employers nationwide. Employee blogs may bring negative publicity to a company, as well as put that company at risk for legal problems such as invasion of privacy, defamation or a violation of state or federal laws.

"Any employer today who is not focused on this latest cyberspace challenge and who is not taking appropriate steps, both to protect the company's interest and not violate their employees' rights in the process, is being foolish," says Lynn C. Outwater, managing partner at Jackson Lewis LLP. "Employers really need to be prepared in a positive, preventive fashion to take on the challenges of blogging."

Smart Business spoke with Outwater about how business owners can protect their companies against the dangers of employee blogging.

Lynn C. Outwater
Managing partner
Jackson Lewis LLP

What are the risks associated with employee blogging?

From an employer perspective, there have been a growing number of bloggers that are now focusing on the workplace. Employers are taking a much closer look at the content of employee blogs and finding that they, the employer, are the subject of the blogs.

Some of the employers have reacted very negatively to this discovery by disciplining or discharging the employee blogger. Some of these actions have become the subject of either employment litigation and/or negative public scrutiny.

For example, in 2004, an airline discharged a flight attendant for allegedly posting suggestive photographs of herself in her airline uniform on her blog. This triggered widespread media coverage — the majority of which depicted the airline negatively — as well as a gender discrimination lawsuit.

Employers are concerned that a blogger might inadvertently or purposely divulge trade secrets or other confidential and proprietary information. This is particularly true with a blog, because anyone can have access to it through the Internet. You don't know who is viewing it or what is being done with the information.

Similarly, a blogger could divulge something seemingly innocuous about daily life as a company employee, which could violate a customer contract, a confidentiality pledge or some third-party agreement, or divulge confidential client information, all of which would be of grave concern to an employer.

Another thing that could happen is the employee might give out corporate information of a nonpublic nature, which could be a violation of federal or state securities laws. Similarly, blogs could also contain information that could expose an employer to liability for defamation, employment discrimination, harassment, breach of privacy, intentional infliction of emotional distress and other common-law or statutory claims.

How can employers protect themselves against the risks of blogging?

We strongly recommend that an employer not automatically discipline or terminate an employee who expresses his or her views in a blog without seeking legal counsel because those that do blog may have certain employee protections.

A blogger who complains on his or her blog about purported company misconduct may qualify for protection under certain state or federal whistleblower laws or the Sarbanes-Oxley Act.

Also, under the federal statute of the National Labor Relations Act, a blogger can discuss the terms, conditions or benefits of his or her employment with other employees. Blogging could be viewed as a protected, concerted activity under this act. As a result, employers should seek counsel before they take adverse action. That is No. 1.

No. 2, they should absolutely draft a blogging policy.

What should employers include in a blogging policy?

It is very important to advise employees of the information about which an employee should not blog. For example, we would recommend an employer tell all employees that no blogging should occur when there is proprietary or confidential information being disclosed or trade secret information being disclosed.

Employees should know that revealing that information is entirely inappropriate.

Second, employers should include a requirement that bloggers refrain from identifying the company's name in their blog. Alternatively, a requirement could be that the blogger post a disclaimer stating that the views expressed in the blog are not necessarily those of, or supported by, the company.

Employees should also be prohibited from using the company's banner, logo or other identifying symbol in their blog.

A third suggestion is that there should be an explicit statement that the company reserves the right to take any action against the employee that it deems appropriate if the blog contains information that violates company policy or is in any way deemed to be harassing, sexually explicit, discriminatory, threatening or intimidating.

Fourth, a statement should be made that the company's equipment, including computers and electronic communication systems, should be limited to company business only.

LYNN C. OUTWATER is a managing partner at Jackson Lewis LLP. Reach her at (412) 232-0232.

Insights Labor & Employment is brought to you by Jackson Lewis LLP

POLICY ON THE USE OF COMPANY'S TECHNOLOGY PLATFORM

OFFICE OF PRIME RESPONSIBILITY

The Director of Information Services shall be responsible for implementing this policy.

1.0 PURPOSE

It is the purpose of the company to utilize various technological tools for the sole purpose of assisting in conducting its business. These tools include, but are not limited to, use of internal and external e-mail, telephones, verifones, facsimiles and personal computers. All computers and communications equipment and facilities, including e-mail, and the data and information stored on them are and remain at all times business property of the company and are to be used for business purposes only.

2.0 SCOPE

This policy is applicable to all categories of employees.

3.0 POLICY

3.1 The electronic mail system and other technology tools of the Company may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

3.2 The technology platform may not be used to create any offensive or disruptive messages. Among those which are consider offensive, are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone s age, sexual orientation, religious or political beliefs, national origin, or disability.

3.3 The technology platform shall not be used to send or receive copyrighted materials, trade secrets proprietary financial information, or similar materials without prior authorization.

3.4 The Company reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail or telephone system for any purpose. Such review or audit will occur at the sole discretion and timing of the Company. The confidentiality of any message should not be assumed.

3.5 Employees shall not use a code, access a file, or retrieve any stored information unless authorized to do so.

4.0 **DISCIPLINARY ACTION**

Any Employee who violates this policy or uses the technology platform for improper purposes shall be subject to discipline, up to and including termination of employment. Disciplinary actions will be viewed in coordination with the Company's General Conduct Policy.

Electronic Media Policy

Personal use of Company's electronic media is discouraged. Company, however, recognizes that personal use of these media will occur, but such use should be kept to a minimum. All personal use must be consistent with Company's policies and the efficient conduct of Company business. Employees must refrain from excessive or irresponsible personal use. Personal use of Company's communication and electronic media resources is strictly prohibited for high-bandwidth usage including: video streaming, music streaming, peer-to-peer file sharing and similar resource-intensive activities.

Company recognizes that use of the Internet and other electronic media has many benefits for the Company and its employees. The Internet and e-mail make communication and research more efficient and effective. However, unacceptable usage of the Internet can place Company and others at risk. This policy discusses acceptable usage of the Internet and other electronic media.

Cell Phone/Personal Digital Assistant (PDA) Usage

1. Cell phones and PDAs should be turned off or set to silent or vibrate mode during meetings, conferences and in other locations where incoming calls may disrupt normal workflow.
2. Employees may carry and use personal cell phones and PDAs while at work so long as personal usage does not unreasonably interfere with productivity. If employee use of a personal cell phone/PDA causes disruptions or loss in productivity, the employee may become subject to disciplinary action per company policy.
3. Personal cell phones and PDAs may be used for company business when necessary (e.g., while out of the office). Employees may be reimbursed for the incoming business calls to their personal cell phones. Employees shall not be reimbursed for outgoing calls made from their cell phones unless prior authorization is obtained from their immediate supervisor.
4. Employees are strongly advised not to use a cell phone or PDA to conduct Company business while operating a motor vehicle unless he/she is using a hands free device. In addition, an employee's use of electronic communication systems while driving must comply with local law as many states prohibit use of cell phones and PDAs while driving.

Telephones

Desktop telephones are provided for conducting Company business. Long distance collect calls should be denied unless approved by a Company Officer.

Personal calls should be kept at a minimum during working hours. Any long distance charges resulting from personal calls made from Company by an employee must be reimbursed to Company.

Telephone calls regarding student records should be referred to the Records Office.

Voice Mail Policy

Every Company employee is responsible for using the Voice Mail system properly and in accordance with this policy. Any questions about this policy should be addressed to the Human Resources Department.

The Voice Mail system has been provided by Company for use in conducting company business. All communications and information transmitted by, received from, or stored in this system are company records and the property of Company. Company, at its discretion as owner of the Voice Mail system, reserves and may exercise the right to monitor, access, retrieve, and delete any matter data stored in, created, received, or sent over the Voice Mail system, for any reason without the permission of any employee and without notice.

Even if employees use a password to access the Voice Mail system, the confidentiality of any message stored in, created, received, or sent from the Company Voice Mail system still cannot be assured. Use of passwords or other security measures does not in any way diminish Company's rights to access materials on its system, or create any privacy rights of employees in the messages and files on the system. Any password used by employees must be revealed to Company upon request as Voice Mail messages may need to be accessed by the Company in an employee's absence.

Even though Company reserves the right to retrieve and review any Voice Mail messages, those messages should still be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or listen to any Voice Mail messages that are not sent to them. Any exception to this policy must receive the prior approval of Company management.

Company's policies against sexual or other harassment apply fully to the Voice Mail system, and any violation of those policies is grounds for discipline up to and including termination of employment. Therefore, no Voice Mail messages should be created, sent, or retained if they contain intimidating, hostile, or offensive material concerning race, color, religion, sex, age, national origin, disability or any other classification protected by law.

The Voice Mail system may not be used to solicit for religious or political causes, commercial enterprises, outside organizations, or other non-job related solicitations except where required by law.

Users should routinely delete outdated or otherwise non-useful Voice Mails. These deletions will help keep the system running smoothly and effectively, as well as minimize maintenance costs.

Because of the storage space required for Voice Mail messages, employees should not send a Voice Mail message to a large number of recipients without prior approval from their supervisor.

Employees are reminded to be courteous to other users of the system and always to conduct themselves in a professional manner. Voice Mails are sometimes misdirected or forwarded and may be heard by persons other than the intended recipient. Users should create Voice Mail communications with no less care, judgment and responsibility than they would use for letters or internal memoranda written on Company letterhead. Employees should also use professional and courteous greetings on their Voice Mail boxes so as to properly represent Company to outside callers.

Because Voice Mail recordings and messages may be subject to discovery in litigation, Company employees are expected to avoid making statements in Voice Mail that would not reflect favorably on the employee or Company.

In order to avoid accidentally disclosing message contents to unauthorized listeners, employees should not listen to Voice Mail messages while using the speaker phone feature.

Any employee who discovers misuse of the Voice Mail system should immediately contact the Human Resources Department. Violations of Company's Voice Mail policy may result in disciplinary action up to and including termination.

E-mail Policy

The following guidelines have been established for using e-mail in an appropriate, ethical and professional manner.

1. The e-mail system is the property of Company. It has been provided by Company for use in conducting company business. All communications and information transmitted by, received from, or stored in this system are company records and the property of Company. Use of the e-mail system for personal purposes should be limited and not interfere with company business or your productivity.
2. The e-mail system shall not be used to send (upload) or receive (download) Company copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization from Company management. If employees are uncertain about whether certain information is copyrighted, proprietary, or otherwise inappropriate for transfer, they should resolve all doubts in favor of not transferring the information and consult the Company Legal Department.
3. Disparaging, abusive, profane, or offensive language; materials that would adversely or negatively reflect upon Company or be contrary to Company best interests; and any illegal activities -- including piracy, cracking, extortion, blackmail, copyright infringement, and unauthorized access to any computer systems are forbidden.
4. Company's policies against sexual or other harassment apply fully to the e-mail system, and any violation of those policies is grounds for discipline up to and including termination of employee. Therefore, no e-mail messages should be created or sent if they contain intimidating, hostile, or offensive material concerning race, color, religion, sex, age, national origin, disability or any other classification protected by law. If you receive such an email, do not forward or retain. Delete such email immediately.
5. Employees may not send chain e-mails or mass mailing e-mails.
6. Employees are reminded to be courteous to other users of the system and always to conduct themselves in a professional manner. E-mails are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient. Users should write e-mail communications with no less care, judgment and responsibility than they would use for letters or internal memoranda written on Company letterhead.

7. Each employee is responsible for the content of all text, audio or images that he/she places or sends over the company's Internet and e-mail system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. Also, be aware that Company's name is attached to all messages so use discretion in formulating messages.
8. Employees may not send Company business e-mails from a personal email account to customers, staff, vendors, or other parties related to Company. In other words, the use of external email or IM services, such as Yahoo or MSN, for conducting any Company business communications is prohibited. All Company business-related e-mail messages **must** be sent from a Company email account. Employees may not access customer, staff, vendor or other e-mail addresses from any Company system for any non-Company business-related purpose.
9. All Company e-mail addresses are Company property and may not be saved, sent, or used for any non-Company business-related purposes.
10. Internal and external e-mail messages are considered business records and may be subject to discovery in the event of litigation. Be aware of this possibility when sending e-mail within and outside the Company.
11. The e-mail system may not be used to solicit for religious or political causes, commercial enterprises, outside organizations, or other non-job related solicitations except where required by law.
12. Any employee who discovers misuse of the e-mail system should immediately contact their supervisor and the Company CIO.
13. Violations of Company's e-mail policy may result in disciplinary action up to and including termination of employment.

Computer Software (Unauthorized Installation and Copying)

Company prohibits the installation and use of unauthorized software on Company's computer systems, PCs, laptops, desktop systems, servers and network attached devices. Only authorized Company IT staff may install software on Company computer systems. Connection of unauthorized devices, including personal PCs, laptops, desktop systems, servers and network devices, to the Company network is strictly prohibited.

Company prohibits the illegal duplication of software. The law protects the exclusive rights of the copyright holder and does not give users the right to copy software. The only exception is the user's right to make a backup copy for archival purposes. Unauthorized duplication of software is a Federal crime. Penalties include fines of as much as $250,000, and jail terms of up to five years.

Internet Usage Policy

Excessive personal use of the Company internet system. You may not use the internet connection excessively for non-business/personal reasons to the detriment of your productivity and efficiency or the productivity of those around you.

Blocking of inappropriate content. Company may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by Company networks. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site.

Prohibited activities. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful, inappropriate, offensive (including offensive material concerning sex, race, color, national origin, religion, age, disability, or other characteristic protected by law), or in violation of Company's equal employment opportunity policy and its policies against sexual or other harassment may not be downloaded from the Internet or displayed or stored in Company's computers. Employees encountering or receiving this kind of material should immediately report the incident to their supervisors or the Human Resources Department. Company's equal employment opportunity policy and its policies against sexual or other harassment apply fully to the use of the Internet and any violation of those policies is grounds for discipline up to and including termination of employment.

Games and entertainment software. Employees should not use the company's Internet connection to download games or other entertainment software or to play games over the Internet.

Virus detection. Files obtained from sources outside Company, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail; and files provided by customers or vendors may contain dangerous computer viruses that may damage Company's computer network. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with Company-approved virus checking software. If you suspect that a virus has been introduced into Company's network, notify the Help Desk immediately.

Copyrighted materials. Any copyrighted materials belonging to entities other than Company may not be transmitted by employees on the company's network. All employees obtaining access to other companies' or individual's materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy to reference only. If you find something on the Internet that may be interesting to others, do not copy it to a network drive. Instead, give the URL (uniform resource locator or "address") to the person who may be interested in the information and have that person look at it on his/her own.

Any employee who abuses the privilege of Company access to the Internet, may be denied access to the Internet and, if appropriate, be subject to disciplinary action up to and including termination.

Recording Devices in the Workplace

Company prohibits employee use of cameras, tape recorders or other recording devices in the workplace as a preventative step believed necessary to secure employee and student privacy, trade secrets and other business information.

1. Employees are prohibited from utilizing cameras or other video or audio recording devices in the workplace unless specific advance written authorization has been obtained from their department head.

2. Authorization may be granted when a specific business purpose will be served by the use of such a device and when its use will not violate employee privacy. In such a case, all parties to the meeting or conversation that is to be recorded must have been informed at its outset that it will be monitored, transcribed, intercepted, or recorded,

and they have consented to such actions prior to the conversation, preferably in writing.

3. Bringing a recording device into the workplace that will not be used for recording, such as a cell phone with a built-in camera, is permissible.

4. Employees are also prohibited from arranging for others, including non-employees, to engage in any recording of conversations, phone calls or other activities in the workplace.

5. Employees should regard this policy as an explicit statement that Company does not consent to tape recording of any meetings or discussions without prior authorization as discussed above.

6. Employees with questions about this policy should contact their supervisor or Human Resources.

Company's Right to Monitor Computer Systems

All company-supplied technology, including computer systems and company-related work records, belong to Company and not the employee. **Therefore, employees have no right of personal privacy in any matter stored in, created, received, or sent over the Company e-mail system or in any matter stored in or created on any Company owned computer or network.**

Company, at its discretion as owner of the systems, reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the e-mail system (or any other Company computer systems), for any reason and without the permission of any employee.

Even if employees use a password to access the e-mail system, the confidentiality of any message stored in, created, received, or sent from the Company e-mail system still cannot be assured. Use of passwords or other security measures does not in any way diminish Company's rights to access materials on its system, or create any privacy rights of employees in the messages and files on the system. Any password used by employees must be revealed to Company upon request as files may need to be accessed by the company in an employee's absence.

Employees should be aware that deletion of any e-mail messages or files will not truly eliminate the messages from the system. All e-mail messages and files may be stored on a central back-up system in the normal course of data management.

Even though Company has the right to retrieve and read any e-mail messages, those messages should still be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages or files that are not sent to them.