MessageLabs®

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

Not Just Words: Enforce Your Email and Web Acceptable Usage Policies

By Nancy Flynn,
Executive Director, The ePolicy Institute
Author, The ePolicy Handbook, E-Mail Rules, Instant Messaging Rules, Blog Rules, Writing Effective E-Mail, and E-Mail Management

Preface

The ePolicy Institute™, www.epolicyinstitute.com, and MessageLabs, www.messagelabs.com, have created this business guide to provide Best-Practices Guidelines for Managing Workplace Email and Web Use to Minimize Risks and Maximize Compliance. Through the implementation of strategic Email and Web Acceptable Usage Policies and Procedures, incorporating clearly written rules, formal employee education, and proven technology solutions, U.S. employers can enhance productivity, cut costs, reduce (and in some cases eliminate) the likelihood of email- and web- related litigation, regulatory investigations, security breaches, and other electronic disasters.

Not Just Words: Enforce Your Email and Web Acceptable Usage Policies is produced as a general best-practices guidebook with the understanding that neither the author, ePolicy Institute Executive Director Nancy Flynn, nor the publisher, MessageLabs, is engaged in rendering advice on legal, regulatory, or other issues. Before acting on any rule, policy, or procedure addressed in **Not Just Words: Enforce Your Email and Web Acceptable Usage Policies**, you should consult with legal counsel or other professionals competent to review the relevant issue.

The ePolicy Institute is a leading source of speaking, training, and consulting services related to workplace email and Internet policies, communication, and management. The ePolicy Institute is dedicated to helping employers limit email and web risks, including litigation and regulatory investigations, while enhancing employees' electronic communication skills. Visit www.epolicyinstitute.com to learn more.

MessageLabs is a leading provider of integrated messaging and web security services, with over 18,000 clients ranging from small business to the Fortune 500 located in more than 86 countries. MessageLabs provides a range of managed security services to protect, control, encrypt and archive communications across Email, Web and Instant Messaging. These services are delivered by MessageLabs globally distributed infrastructure and supported 24/7 by security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information.

Table of Contents

Email & Web Rule #1:

Litigation and Regulations, Productivity and Security Create the Need for Strategic Email and Web Management

Employee use of the company computer system can open any organization to potentially costly and protracted risks including litigation, regulatory investigations, security breaches, malicious intruder attacks, lost productivity, business interruptions, and public embarrassment should a workplace lawsuit be filed or the media get wind of a particularly salacious electronic disaster story.

You cannot be present in every office on every floor of every facility every hour of every day. You cannot rely on managers and staff to exercise sound judgment and good taste 100% of the time. And you should not discount the damage external intruders and internal saboteurs pose to your organization.

- Should a female employee walk into the office of a male associate who, at that moment, is viewing pornography on his laptop, you, the employer, could wind up on the wrong side of a sexual harassment or hostile work environment claim.

- If a former employee subpoenas company email and other electronically stored information in the course of a workplace lawsuit, your organization could face a lengthy and expensive search for messages, attachments, and other data.

- Were a disgruntled employee of your publicly traded company to jump the gun and forward confidential financial data to the business media, you could find yourself in violation of security laws and facing the scrutiny of Wall Street and the possibility of a stock decline.

- If a malicious intruder unleashed malware, spyware, or a virus on your system, you could lose valuable intellectual property and other confidential information, resulting in lost productivity, sales, and professional credibility.

Best Practice: For employers who are eager to reduce business and security risks associated with electronic communication, there is a solution. Implement a clear and effective email and web acceptable usage policy (AUP) enforced by proven technology - —and watch electronic threats decrease as compliance with organizational, legal, and regulatory rules increases.

Email & Web Rule #2:

Apply Policy, Training and Technology to Help Manage Email and Web Risks

For responsible organizations operating in the age of email and the web, acceptable usage policies are essential business tools. Clearly written and effectively communicated email and web AUPs can help employers minimize risks, maximize compliance, and demonstrate to courts and regulators that the organization has done its due diligence, making every effort to manage electronic use, content, and threats.

Best Practice: Many employers find the best way to manage people problems is through the application of technology solutions. If you have implemented email and web acceptable usage policies, but are struggling to find the necessary tools to enforce them, visit Messagelabs at www.messageLabs.com to review policy-based management and monitoring technology solutions for email and web. These solutions are designed to help maximize productivity while minimizing workplace risks.

Email & Web Rule #3:

The Easiest Way to Control Email Risk Is to Control Written Content

When it comes to inappropriate content and offensive language, employers have little tolerance. Of the 28% of managers who fired workers for email violations in 2007, more than half (62%) cited inappropriate content or off-color language as the termination-worthy offense—up from just 8% six years earlier.[1]

Use written acceptable usage policy to notify employees that compliance with email content rules is 100% mandatory. Ban obscene, pornographic, sexual, harassing, discriminatory, defamatory, menacing, and threatening language. Prohibit the transmission of gossip, rumors, jokes, or disparaging remarks about executives, coworkers, or outside parties.

Impose rules designed to protect the company's confidential data, trade secrets, intellectual property, and internal documents including in-house email. For public companies and regulated firms, it is particularly important that email be managed in accordance with the organization's acceptable usage policy and regulators' content rules. Unmanaged confidential content could land a publicly traded company in hot water with the SEC, exposing the company to liability for violations of federal securities laws. From securities fraud, to jumping the gun, selective disclosure, and forward-looking statements, public companies must ensure that employees do not use email to disclose proprietary insider information, transmit untrue content, or otherwise violate securities laws.[2]

Best Practice: For public companies and regulated firms, it is particularly important that email and web usage is managed in accordance with the company's written acceptable usage policies and regulators' content rules. Support organizational rules with MessageLabs services designed to automatically and quickly scan email for potentially costly violations.

Real-Life Email Content Disaster Story:

Top Secret $1 Billion Settlement Talks Exposed by Email [3]

Need proof that email is a risky way to transmit confidential information? Eli Lilly and its outside legal counsel learned that lesson the hard way in January 2008, when *The New York Times* broke the story of Lilly's confidential settlement talks with the U.S. government—thanks to a misaddressed top-secret email message.

Eli Lilly and federal prosecutors were in settlement talks related to civil and criminal investigations into the marketing of the antipsychotic drug Zyprexa. With negotiations over Lilly's alleged marketing improprieties reaching more than $1 billion (in addition to the $1.2 billion Lilly had already paid to settle 30,000 individual lawsuits), the pharmaceutical giant was eager to keep the settlement talks under wraps.

Given the secrecy surrounding the negotiations, company officials were understandably shocked when contacted by a reporter preparing to publish an in-depth article exposing the Zyprexa settlement details on the front page of *The New York Times*. Lilly initially accused federal prosecutors of leaking the news. As it turns out, the source of the leak was much closer to home.

One of Lilly's lawyers at the Philadelphia-based firm Pepper Hamilton had intended to email a confidential settlement document to attorney Bradford Berenson, her co-counsel at Lilly's Chicago law firm Sidley Austin. Unfortunately, she mistakenly sent the top-secret document to *New York Times* reporter Alex Berenson, whose name was the first to pop up on the sender's email autocomplete feature when she began typing *Berenson*[4]. Click. Eli Lilly's private, closed-door negotiations went public on the front page of The New York Times, thanks to a misaddressed top-secret email message.

Support written acceptable usage policies with formal employee education designed to inform users of email- and web- related risks and regulations, policies and procedures. At the conclusion of training, have all employees sign and date an acknowledgement form confirming that they have read the company's email and web policies, understand the rules, and agree to comply with acceptable usage policies or accept the consequences, up to and including termination.

Email & Web Rule #4:

Combine Policy with URL Blocks to Protect Resources, Preserve Productivity and Prevent Lawsuits

Of the 30% of bosses who terminated employees for web violations in 2007, fully 84% cited the viewing, downloading, or uploading of pornography and otherwise offensive or inappropriate material as the reason. That's a 65% increase over 2001, according to American Management Association/ePolicy Institute research.[5] Use written acceptable usage policy to remind employee-surfers to steer clear of any websites that the organization has ruled off-limits.

Use acceptable usage policies to notify employees that they are prohibited from viewing, downloading, uploading, forwarding, printing, copying, or filing sexually explicit or otherwise objectionable, non-business-related web content. Outlaw wasteful and potentially risky activities including dating online, playing games, participating in chat rooms, gambling, shopping, and downloading streaming audio, video, and other bandwidth-wasting files. Support written web rules — and enforce employee compliance — with an employee training program backed by policy-based monitoring and management technology solutions designed to review and restrict inappropriate online behavior.

To maximize compliance with acceptable usage policy and content rules, take advantage of URL filtering technology from MessageLabs Web Security Services. Fully 96% of employers who block web access are concerned about employees visiting adult sites with sexual, romantic, or pornographic content. Companies also use URL blocks to stop users from visiting game sites (61%); social networking sites (50%); entertainment sites (40%); shopping and auction sites (27%); sports sites (21%); and external blogs (18%), according to the *2007 Electronic Monitoring & Surveillance Survey* from American Management Association and The ePolicy Institute.[6]

Real-Life Email Content Disaster Story:
Government Employees Prefer Porn to Productivity

An investigation into District of Columbia government agencies revealed that nine employees had each surfed at least 20,000 porn sites (about 200 hits per workday) during 2007. In addition, another government employee had visited more than 48,000 pornographic sites during the same 12-month period. Prompted by an employee's complaint about the pervasive browsing and downloading of pornographic images, the investigation led to disciplinary action, ranging from two-week suspensions to terminations, against 32 employees from a dozen District agencies.[7]

Best Practice: Don't let thoughtless leaks, irresponsible content, or inappropriate surfing sink your corporate ship. Institute written acceptable usage policies that clearly spell out what material may and may not be transmitted, acquired, viewed, downloaded, or uploaded via email or the web. Support your policies with employee education backed by MessageLabs services.

Email & Web Rule #5:
Personal Use Heightens Organizational Risk

The 58% of employers who dismissed employees in 2007 for computer violations cited excessive personal email (26%) or web (34%) use as the reason.[8] Excessive personal use takes a toll on employee productivity, eats up valuable system space, and creates potentially damaging legal evidence:

- 86% of employees engage in personal email at work, with 10% spending four or more hours a day emailing, according to American Management Association/ePolicy Institute research.[9]

- Personal content tends to be more relaxed — thus potentially more risky — than business-related content.

- Personal email messages that are retained and archived alongside business records may become part of the evidence pool during litigation, possibly disgracing employees and derailing the organization's legal position in the process.

- Personal web surfing leaves electronic footprints that computer forensic experts will happily follow in the course of legal discovery.

Real-Life Email Content Disaster Story:
Prosecutor's Love Life Exposed [10]

Texas' most powerful prosecutor, the district attorney of Harris County (population 4 million), faced public embarrassment, family strife, media scrutiny, and political disaster when private email correspondence was inadvertently made public by a federal court in December 2007.

District Attorney Charles A. Rosenthal, Jr. used his office email system to send hundreds of personal messages including racist jokes, pornographic images, and what *The New York Times* called "professions of love and longing" to his executive secretary. The married DA's private email messages, which were revealed as part of a federal civil rights lawsuit against Harris County, initially had been sealed to prevent public exposure. When a court mix-up inadvertently unsealed the messages, Rosenthal's personal dirty laundry was exposed, placing him under intense government, media, family, and public scrutiny for misusing his county email account.[11]

Rosenthal's electronic disaster escalated when he admitted to a federal judge that, in violation of two subpoenas and a court order, he had deleted as many as 3,500 email messages related to the civil rights lawsuit. In the process, Rosenthal opened himself to possible perjury charges. Ultimately, Rosenthal's email disaster led to his resignation from office.[12]

Best Practice: Manage personal email and web usage with clear rules. If you allow personal use in the office, be sure to let users know exactly when personal emailing and web surfing is allowed, for how long, during what periods of the day, and under what circumstances. Clearly written rules are easier to understand and adhere to than vague suggestions. If "some" personal use is allowed, for example, employees will have to individually interpret where the line is drawn, and you may not be comfortable with their conclusions.

Email & Web Rule #6:
Exercise Your Legal Right to Monitor — and Discipline — Employees

The federal Electronic Communications Privacy Act (ECPA) makes it clear that a company-provided computer system is the property of the employer. U.S. employers have the legal right to monitor all employee computer activity, transmissions, and content—including incoming, outgoing, and internal email messages, as well as web surfing, downloads, and uploads.

When it comes to computer monitoring, employers are primarily concerned about inappropriate web surfing, with 66% reviewing Internet connections, and another 45% tracking content, keystrokes, and time spent at the keyboard. In addition, 43% of bosses monitor employee email, either taking advantage of technology to accomplish the job automatically (73%) or assigning an individual to manually read and review messages (40%), according to the *2007 Electronic Monitoring and Surveillance Survey* from American Management Association and The ePolicy Institute.[13]

Unfortunately, employers often turn a blind eye to internal email. While 96% of the companies that monitor email review external (incoming and outgoing) messages, only 58% monitor the internal email conversations that take place among employees.[14]

Real-Life Email Content Disaster Story:
Economist's Email Slams Singapore [15]

Morgan Stanley's chief Asia economist, Andy Xie, was forced to resign after colleagues circulated a caustic internal email that Xie had intended strictly for readers inside Morgan Stanley. Xie's email was so highly critical of Singapore that it incited the wrath of the city-state, a Morgan Stanley client.

In his internal message to colleagues, Xie sniped, *"Singapore's success came mainly from being the money-laundering centre for corrupt Indonesian businessmen and government officials." And "Singapore isn't doing well. To sustain its economy, Singapore is building casinos to attract corrupt money from China."*[16]

In addition to terminating Xie and the two staffers who leaked his internal email, Morgan Stanley was forced to smooth over relations with the sensitive Singaporean government and endure a public relations nightmare culminating in worldwide publicity about the fallout from Xie's inflammatory internal email.[17]

Best Practice: Use MessageLabs services to audit employees' email communications and web browsing. Using a policy-based, automated search tool, employers can seek out target words and phrases including the names of company executives, products, trade secrets, competitors, customers, or patients. In addition, the organization can use the same technology to capture and block obscene, harassing, discriminatory, or otherwise offensive or objectionable content that could potentially trigger a hostile work environment, harassment, or discrimination claim. Monitoring technology also can be used to spot and stop transmission of particularly large attachments, which may contain valuable data and always warrant a review.

Email & Web Rule #7:
Employees Have Absolutely No Reasonable Expectation of Privacy

Employees often are surprised to learn that they have absolutely no reasonable expectation of privacy when using the company computer system to transmit email, surf the web, or engage in other forms of electronic communication, business-related or personal.

Private employers operating in employment-at-will states (which most states are) have the right to fire employees for just about any reason—including accidental and intentional email violations and inappropriate Internet use. The 28% of organizations that fired employees for email misuse in 2007 cited the following as termination-worthy reasons: violation of any company policy including email rules, ethics guidelines, or harassment/discrimination policy (64%); inappropriate or offensive language (62%); excessive personal use of the email system (26%); breach of confidentiality rules (22%); other violations, accidental or intentional (9%).

The 30% of bosses who fired workers for Internet misuse cited the following reasons: viewing, downloading, or uploading inappropriate/offensive content (84%); violation of any company policy (48%); excessive personal use (34%); other (9%).[18]

In addition to employers, law enforcement agencies, courts, regulators, the media, the public, message recipients and their employers are likely to access, review, retain, and permanently archive your email transmissions and history of Internet surfing. Consider the following:

- The Federal Rules of Civil Procedure and similar state laws make email and other electronically stored information available to courts, lawyers, investigators, jurors, and witnesses in the course of litigation.
- Email is the electronic equivalent of DNA evidence. Fully 24% of employers have had employee email subpoenaed by a court or regulator, and another 15% have gone to court to battle workplace lawsuits triggered by employee email.[19]
- State and federal Freedom of Information statutes give the media and taxpayers access to government employees' email messages and attachments.
- The Patriot Act authorizes law enforcement to seize corporate email, and employers are under no obligation to notify users that their messages are under review.

- SOX, GLBA, HIPAA, NYSE, SEC, NASD, and the IRS are just a few of the government and industry regulations and regulators that audit email.

- Copied, forwarded, and improperly addressed “eyes only” email can easily land in the inboxes of clients, competitors, coworkers, the media, and other unintended and uninvited internal and external readers.

- Business record email is likely to be retained and archived by clients, prospects, suppliers, business partners, and other third-parties with whom you, your colleagues and staff communicate.

Best Practice: While the Electronic Communications Privacy Act gives employers the right to monitor all email transmissions and web activity that take place on the organization’s system, only two states (Delaware and Connecticut) require employers to inform employees that they are being monitored. Nonetheless, it is a good idea for all employers to inform employees that they have no reasonable expectation of privacy when using the Internet system. Combat resentment and invasion of privacy claims by taking time to explain why you monitor, how monitoring works, what management is looking for, why policy compliance is mandatory, and what type of penalties await those who violate acceptable usage policies.

Email & Web Rule #8:

Lock Out Malicious Intruders to Keep Your Secrets Safe and System

From viruses, spammers and scammers to phishing, Trojans and spyware—the invisible bad guys who inhabit the Internet are committed to infiltrating your system, disrupting your business, stealing your confidential data, and damaging your resources and reputation.

When it comes to email and web threats, regulated firms have particular cause for alarm. For example, businesses that are regulated by the Sarbanes-Oxley Act (SOX) or the Gramm-Leach-Bliley Act (GLBA) are obligated to ensure that financial data and related documents—including confidential internal memos, revenue projections, or other content transmitted via email—are effectively protected from malware, viruses, and other malicious intruders. Similarly, health care companies are legally required by the Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy of patient information. HIPAA requires healthcare organizations and their suppliers to safeguard email messages and attachments that contain protected health information (PHI) related to a patient’s health status, medical care, treatment plans, and payment issues. Failure to do so can result in seven-figure regulatory fines, civil litigation, criminal charges, and jail time.

Use a combination of acceptable usage policy, training, and technology to lock out malicious intruders—and keep your secrets safe and your system secure.

Best Practice: Combine written rules and employee education to alert users to specific email and web threats—and the individual roles they play in protecting the company and business-critical data from data thieves, external intruders, internal saboteurs, and other enemies. Trust MessageLabs Email Anti-Virus, Anti-Spam, Content Control, Image Control, URL Filtering, and Web Security Services to uncover and intercept known and unknown email and web threats—before they reach your network and wreak havoc on your people and products, system and services.

Email & Web Rule #9:

Conduct an Annual — Legal-- Review of Email and Web Policies

Review and update email and web acceptable usage policies (AUPs) annually. To be effective, policies must address all current and emerging risks, regulations, laws, and technologies. Before introducing email and web acceptable usage policies to employees, be sure to have your legal counsel review and sign off on each policy. Make sure they address every potential risk facing your organization and industry and are in compliance with federal and state laws governing monitoring and privacy. If you operate within a regulated industry, ensure that your policies comply with regulatory rules. Make sure policies are clearly written and training programs effectively communicate the company’s policies and procedures.

Enforce AUPs with consistent disciplinary action. Use your formal training program to let employees know what type of penalties—up to and including termination—await policy violators. When it comes to discipline, be fair and consistent. Apply established penalties for all policy violations, regardless of the offending party’s rank, title, years of service, or popularity. When it comes to policy compliance, a penalty is a penalty.

Best Practice: Your up-front investment in an annual legal review of email and web acceptable usage policies will pay huge dividends should you one day be hit with a legal claim or regulatory audit. An annual policy review will help establish the fact that your organization has applied best practices and made every effort to keep employees legally compliant.

Sample Email Policy[20]

The company provides employees with electronic business communication tools, including an Email System. This written Email Acceptable Usage Policy governs employees' use of the company's Email System at headquarters and district offices, as well as at remote locations including but not limited to employees' homes, client offices, supplier offices, hotels, and airports.

The company's Email Acceptable Usage Policy applies to employees' use of desktop computers, laptops, Blackberry Smartphones, cellphones, and other hand-held devices, whether provided by the company or owned by the employee or a third party. The company's Email Acceptable Usage Policy applies to full-time employees, part-time employees, independent contractors, interns, consultants, agents, and third parties including but not limited to suppliers and clients.

Any employee who violates the company's Email Acceptable Usage Policy is subject to disciplinary action, up to and including termination.

1.Email Exists for Business Purposes
The Email System is provided primarily for business purposes. Employees may use the company's Email System for personal use strictly in accordance with this policy.

2.Authorized Personal Use of the Email System
Employees may use the Email System to communicate with spouses, children, domestic partners, and other family members. Employees' personal use of the company's Email System is limited to lunch breaks and work breaks only. Employees may not use the company's Email System during otherwise productive business hours.

Employees who need to hold personal communications with persons other than spouses, children, domestic partners, and other family members via the company's Email System must first obtain permission from management.

Employees are prohibited from using the Email System to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for religious or other personal causes.

Employees are prohibited from using the Email System to play online games, visit chat rooms, shop online, or engage in illegal activity including but not limited to gambling and drug dealing.

3.Personal Email Tools and Accounts Banned
Employees are prohibited from using personal web-based email accounts (Gmail, AOL, etc.) for business or personal communications.

4.Employees Have No Reasonable Expectation of Privacy
The Email System is the property of the company. All passwords, user IDs, and messages created and transmitted are the property of the company. The company reserves the right to monitor all email transmissions conducted via the company's computer system. Employees have no reasonable expectation of privacy when it comes to business and personal use of the company's Email System. The federal Electronic Communications Privacy Act gives management the legal right to access and disclose all employee email transmissions. All employee email messages (incoming, outgoing, and internal) will be monitored. The company reserves the right to monitor, inspect, copy, review, and store at any time and without notice any and all usage of the company's Email System, and any and all files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with employee usage. Management reserves the right to disclose email text and images to regulators, the courts, law enforcement, and other third parties without the employee's consent.

5. Prohibited Use of the Email System: Offensive Content and Harassing/Discriminatory Activities Are Banned

Company employees have the right to work in an environment that is free from hostility of any kind. Employees are prohibited from using the Email System to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive. Employees are prohibited from using the Email System to:

- Send, receive, solicit, print, copy, or reply to text or images that disparage others based on their race, religion, color, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

- Send, receive, solicit, print, copy, or reply to jokes (text or images) based on sex, sexual orientation, race, age, religion, national origin, veteran status, ancestry, or disability.

- Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.

- Spread gossip, rumors, and innuendos about employees, clients, suppliers, or other outside parties.

- Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.

- Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, off-color, or adult-oriented language.

- Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass the firm, negatively impact employee productivity, or harm employee morale.

6. Confidential, Proprietary, and Personal Information Must Be Protected

Unless authorized to do so, employees are prohibited from using the Email System to transmit confidential firm information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about the firm, employees, clients, suppliers, and other business associates and partners.

Confidential information includes but is not limited to client lists, confidential financial data, credit card numbers, Social Security numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass the company and/or employees were it to be made public.

Employees also are prohibited from using the Email System to transmit copyright-protected information without permission of the copyright holder.

7. Handling Unsolicited Email that Violates Company Policy

The Email Acceptable Usage Policy prohibits employees from sending inappropriate or offensive material. Employees also are prohibited from receiving material that violates the company's Email Acceptable Usage Policy. In the event that an employee receives email messages that violate policy, the employee is to take the following steps:

(a) If You Know the Sender: If an employee receives email that violates firm policy, and the employee knows the sender, then the employee must immediately instruct the sender to stop sending this type of material.

(b) If You Don't Know the Sender: If an employee receives email that violates firm policy, and the employee does not know the sender, the employee should not respond or reply to the message. Instead, the employee should immediately notify the IT manager, who will attempt to block receipt of this type of material in the future.

Employees who follow these procedures will not be deemed to have violated policy. Employees who fail to follow these rules and continue to receive banned material may be deemed to be policy violators and may be disciplined or terminated for violating the company's Email Acceptable Usage Policy.

8.Passwords

Email passwords are the property of the company. Employees are required to provide the CIO with current passwords and user IDs. Only authorized personnel are permitted to use passwords or user IDs to access another employee's email without consent. Misuse of passwords/user IDs, the sharing of passwords/user IDs with non-employees, and/or the unauthorized use of another employee's password/user ID will result in disciplinary action, up to and including termination.

9.Writing Style & Netiquette

Email messages should be treated as formal business documents, written in accordance with the company's Electronic Writing Style Guidelines. Style, spelling, grammar, language, and punctuation should be business-appropriate and accurate. The rules of electronic etiquette, as detailed in the firm's Netiquette Policy, must be adhered to.

10. Email Blasts

Employees are prohibited from sending organization-wide email messages to all employees without approval from the IT department. Employees are prohibited from sending email blasts (mass mailings) to external parties without approval from the IT department. Only the Chief Information Officer and/or Systems Administrator may generate public email distribution lists (email blasts). Employees are prohibited from requesting email replies to organization-wide email or external email blasts without permission from the IT department.

Violations

These guidelines are intended to provide company employees with general examples of acceptable and unacceptable use of the firm's Email System. A violation of this policy may result in disciplinary action up to and including termination.

Acknowledgement

If you have questions about the above Email Acceptable Usage Policy, address them to the Chief Information Officer before signing the following agreement.

I have read the company's Email Acceptable Usage Policy and agree to abide by it. I understand that a violation of any of the above rules and procedures may result in disciplinary action, up to and including my termination.

____

Employee Name (Printed)   Employee Signature

____

Date

Sample Email Policy excerpted from Nancy Flynn, ***The ePolicy Handbook, 2nd Edition***, New York, AMACOM, 2008. For informational purposes only. No reliance should be placed on this policy without the advice of legal counsel. Individual electronic business communication policies should be developed with assistance from competent legal counsel.

Sample Web Policy[21]

(Organization) provides employees with a network connection and web access. This Web Acceptable Usage Policy governs all use of (Organization's) network and web access at headquarters, remote offices, hotels, airports, employees' homes, and any other location.

The (Organization) network and web access are intended for business use only. Employees may access the Internet for personal use only during non-working hours, and strictly in compliance with the terms of this Acceptable Usage Policy.

All information created, transmitted, acquired, downloaded, or uploaded via the organization's network and Internet system is the property of (Organization). Employees should have no expectation of privacy regarding this information. The organization reserves the right to access, read, review, monitor, and copy all messages and files on its computer system at any time and without notice. When deemed necessary, the organization may disclose text or images to law enforcement agencies, regulatory bodies, courts, and other third parties without the employee's consent.

No employee may use a password unless it has been disclosed in writing to (Organization's) Chief Information Officer.

Alternate Internet Service Provider connections to (Organization's) internal network are not permitted unless expressly authorized by the organization and properly protected by a firewall or other appropriate security device(s).

Files downloaded from the web may not be viewed or opened until scanned with virus detection technology. Employees are reminded that information obtained from the web is not always reliable and should be verified for accuracy before it is used.

Prohibited Activities
Employees are prohibited from using (Organization's) network or Internet access for the following activities:

1. Downloading software without the prior written approval of (Organization's) Chief Information Officer. (See Organization's Software Usage Policy.)

2. Disseminating or printing copyrighted materials, including articles and software, in violation of copyright laws.

3. Sending, receiving, printing, or otherwise disseminating Organization's proprietary data, trade secrets, or other confidential information in violation of organization policy or written agreements.

4. Operating a business, usurping business opportunities, soliciting money for personal gain, or searching for jobs outside Organization.

5. Making offensive or harassing statements and/or disparaging others based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

6. Viewing, downloading, uploading, sending, or soliciting sexually oriented messages or images.

7. Visiting websites featuring pornography, terrorism, espionage, theft, or drugs.

8. Gambling or engaging in any other criminal activity in violation of local, state, or federal law.

9. Engaging in unethical activities or content.

10. Participating in activities, viewing, or writing content that could damage Organization's professional reputation.

Compliance & Violations

1. Managers are responsible for ensuring employee compliance with this Web Acceptable Usage Policy.

2. Employees who learn of web policy violations should notify Organization's Chief Information Officer or Human Resources Director.

Employees who violate this policy or use Organization's network or Internet system/access for improper purposes will subject to discipline, up to and including termination.

Acknowledgement

If you have questions about the above Web Acceptable Usage Policy, address them to the Chief Information Officer before signing the following agreement.

I have read the Company's Web Acceptable Policy, and agree to abide by it. I understand that a violation of any of the above rules, policies, and procedures may result in disciplinary action, up to and including my termination.

____

User Name User Signature

____

Date

Sample Web Policy excerpted from Nancy Flynn, ***The ePolicy Handbook, 2nd Edition***, New York, AMACOM, 2008. For informational purposes only. No reliance should be placed on this policy without the advice of legal counsel. Individual electronic business communication policies should be developed with assistance from competent legal counsel.

About The ePolicy Institute™

www.epolicyinstitute.com

The ePolicy Institute is dedicated to helping employers limit email- and web- related risks, including litigation, through effective email and Internet policies and training programs. The author of 10 books published in 5 languages, including E-Mail Rules, Blog Rules, Instant Messaging Rules, The ePolicy Handbook, E-Mail Management and Writing Effective E-Mail, ePolicy Institute Executive Director Nancy Flynn is a popular speaker, trainer, and seminar leader with clients worldwide. She also serves as an expert witness in email- and Internet- related litigation. Since 2001, The ePolicy Institute has collaborated with American Management Association on an annual survey of workplace email and Internet policies, monitoring procedures, and best practices. A popular media source, Nancy Flynn has been interviewed by thousands of media outlets including Fortune, Forbes, Time, NewsWeek, BusinessWeek, Wall Street Journal, US News & World Report, USA Today, Readers' Digest, National Public Radio, CBS Early Show, CNBC, CNN Headline News, CNN Anderson Cooper 360, Fox Business News, NBC and ABC.

Not Just Words: Enforce Your Email and Web Acceptable Usage Policies is based on material excerpted from Nancy Flynn's books The ePolicy Handbook, E-Mail Rules, Instant Messaging Rules, Blog Rules, Writing Effective E-Mail, and E-Mail Management. Contact Nancy Flynn about ePolicy Institute training and consulting, products and services (614-451-3200) or nancy@epolicyinstitute.com.

About MessageLabs

www.messagelabs.com

MessageLabs provides a range of managed services to protect, control, encrypt and archive electronic communications. Listed as a leader in the Gartner Magic Quadrant and many other analyst reports and with more than 18,000 clients ranging from small business to the Fortune 500 located in more than 86 countries, MessageLabs is widely recognized as a market leader in the messaging and web security market.

MessageLabs provides a highly effective and integrated set of on-demand services, to stop both known and unknown threats before they reach your corporate boundaries, address a range of content management challenges and provide around the clock protection for your company. Without the need for hardware or software, MessageLabs services can be deployed anywhere in the world in a matter of minutes. Completely integrated across a global platform, our services for email, web and IM, offer a 'one window' management interface and 24/7 worldwide service and support from our team of security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information.

References

1 2007 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute Survey results available at www.epolicyinstitute.com.

2 Excerpted from Nancy Flynn's telephone interview with Attorney Stephen M. Fronk, Howard Rice Nemerovski Canady Falk & Rabkin, http://www.howardrice.com (October 12, 2005). See also Nancy Flynn, Blog Rules, New York, AMACOM, 2006.

3 "Real-Life Email Content Disaster Story: Top Secret $1 Billion Settlement Talks Exposed by Email" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, AMACOM, 2008.

4 Alex Berenson, "Lilly Considers $1 Billion Fine to Settle Case," The New York Times (January 31, 2008), www.nytimes.com/2008/01/31/business/31drug.html. See also Ina Fried, "The High Cost of E-Mail Autocomplete," CNETNews.com (February 5, 2008), www.news.com/8301-138603-9865371-56.html. See also Katherine Eban, "Lilly's $1 Billion E-Mailstrom," Conde Nast Portfolio.com (February 5, 2008), www.portfolio.com/news-markets/top-5/20008/02/05/Eli-Lilly-E-Mail-to-New-York-T.

5 2007 Electronic Monitoring and Surveillance Survey from American Management Association and The ePolicy Institute and 2001 Electronic Policies and Practices Survey from American Management Association and The ePolicy Institute. Survey results available at www.epolicyinstitute.com.

6 2007 Electronic Monitoring and Surveillance Survey from American Management Association and The ePolicy Institute. Survey results available at www.epolicyinstitute.com.

7 "Real-Life Web Disaster Story: Government Employees Prefer Porn to Productivity" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, AMACOM, 2008. See also "Nine D.C. Employees to Be Fired Over Porn at Work," NBC4.com (January 23, 2008).

8 2007 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute. Survey results available at www.epolicyinstitute.com.

9 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute. Survey results available at www.epolicyinstitute.com.

10 "Real-Life Email Disaster Story: Prosecutor's Love Life Exposed" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, 2008, AMACOM.

11 Ralph Blumenthal, "Prosecutor, Under Fire, Steps Down in Houston" The New York Times (February 16, 2008).

12 Ralph Blumenthal, "Houston Prosecutor Admits He Deleted E-Mail Messages," The New York Times (February 2, 2008).

13 2007 Electronic Monitoring and Surveillance Survey from American Management Association and The ePolicy Institute. Survey results available online at www.epolicyinstitute.com.

14 Ibid.

15. "Real-Life Internal Email Disaster Story: Economist's Email Slams Singapore" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, AMACOM, 2008.

16. Liz Chong, "Two More Morgan Stanley Staff Quit Over Leaked E-Mail," TimesOnline (October 14, 2006), http://business.timesonline.co.uk/tol/business/industrysectors/bankingandfinancial/articl.

17. Liz Chong, "Two More Morgan Stanley Staff Quit Over Leaked E-Mail," TimesOnline (October 14, 2006), http://business.timesonline.co.uk/tol/business/industrysectors/bankingandfinancial/articl. See also Sundeep Tucker, 'Morgan Star Quits After E-Mail Blast," The Australian News (October 5, 2006), www.theaustralian.news.com.au/story/0,20867,20526011-36375,00.html. See also "A Banking Star's Inconvenient Singaporean Truth, 'Asia Sentinel (October 4, 2006), www.asiasentinel.com/index2.php?option=comcontent&task=view&id=199&pop.

18. 2007 Electronic Monitoring and Surveillance Survey from American Management Association and The ePolicy Institute. Survey results available online at www.epolicyinstitute.com.

19. 2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association and The ePolicy Institute. Survey results available online at www.epolicyinstitute.com

20. "Sample E-Mail Policy" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, AMACOM, 2008.

21. "Sample Web Policy" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, AMACOM, 2008.

MessageLabs is widely recognized as a market leader in the messaging and web security market.

MessageLabs®

The ePolicy INSTITUTE™

www.ePolicyInstitute.com