MessageLabs®

Be certain

Ten Easy Steps for Email and Web Best Practices

E-Mail Rules, Instant Messaging Rules, Blog Rules, The ePolicy Handbook, Writing Effective E-Mail, E-Mail Management

A MessageLabs White Paper By Nancy Flynn, Executive Director, The ePolicy Institute Author, *E-Mail Rules, Instant Messaging Rules, Blog Rules, The ePolicy Handbook, Writing Effective E-Mail, E-Mail Management*

Table of Contents

Preface

The ePolicy Institute™, www.epolicyinstitute.com, and MessageLabs, www.messagelabs.com, have created this business guide to provide best-practices guidelines for developing and implementing effective Email and Web Acceptable Usage Policies for the US workplace. Through the implementation of clearly written Acceptable Usage Policies, employers in the US can maximize employee compliance while minimizing the likelihood of litigation, regulatory investigations, security breaches, malicious intruders, and other electronic disasters.

The ePolicy Institute/MessageLabs Guidebook, ***Ten Easy Steps for Email & Web Best Practices***, is produced as a general best-practices guide with the understanding that neither the author (Nancy Flynn, Executive Director of The ePolicy Institute), nor the publisher (MessageLabs) is engaged in rendering advice on legal, regulatory, or other issues. Before acting on any issue, rule, or policy addressed in ***Ten Easy Steps for Email & Web Best Practices***, you should consult with legal counsel or other professionals competent to review the relevant issue.

Ten Easy Steps for Email & Web Best Practices is based on material excerpted from author Nancy Flynn's books *E-Mail Rules, Blog Rules, Instant Messaging Rules, The ePolicy Handbook, Writing Effective E-Mail, and E-Mail Management*.

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

...any time you allow employees to access the Web and e-mail, you put your organization's assets, future, and reputation at risk.

Why Establish Acceptable Usage Policies Governing Email & Web Use and Content?

Whether your organization is a mid-sized company, a small family business, or a publicly traded corporation, any time you allow employees to access the Web and email, you put your organization's assets, future, and reputation at risk. Accidental misuse—and intentional abuse—of email and the Internet can create potentially costly and time-consuming legal, regulatory, security, and productivity headaches for employers of all sizes in all industries.

Best Advice: Manage your organization's email and Web liabilities today with clearly written Acceptable Usage Policies supported by comprehensive, companywide employee training and policy-based monitoring and management technology tools—or risk potentially costly and protracted disaster tomorrow.

Put Best Practices to Work With Policy, Training, and Technology

Organizations that are committed to preventing accidental and intentional email and Web disasters put best practices to work by combining the "***3-Es***" of electronic risk management: (1) **E**stablish policy; (2) **E**ducate the workforce; (3) **E**nforce policy with discipline and technology.

1. Establish comprehensive, clearly written email and Web Acceptable Usage Policies for all employees, from entry-level staff to senior executives. Make sure Acceptable Usage Policies are easy for employees to access, understand, and adhere to. Avoid vague language that leaves policies open to individual interpretation. Update email and Web Acceptable Usage Policies annually to ensure that you respond to evolving laws governing privacy and the Internet; address "emerging" technologies like instant messaging; and adhere to regulatory rules impacting your business and industry.

ePolicy Tip: Because some employees tend to play it "fast and loose" with language and content when emailing friends and family, be sure to incorporate rules governing personal email use in your Acceptable Usage Policy. According to American Management Association/ePolicy Institute research, fully 86% of employees engage in personal email at work. Use your written policy to spell out exactly how much personal email is allowed, when, with whom, under what circumstances, and for how long. Use clear language to communicate specific personal use guidelines. Don't leave room for individual interpretation by employees who might be tempted to engage in excessive personal correspondence on company time.

2. Educate Employees. Don't take employee compliance for granted. Join the 42% of US employers who formally introduce Acceptable Usage Policies during mandatory training covering email and Web risks, rights, rules, regulations, and responsibilities. For a large or geographically disperse workforce, consider a combination of on-site, online, and video training sessions. Build quizzes into training to certify that employees have participated, understand the risks and rules, and agree to comply with email and Web Acceptable Usage Policies—or accept the consequences up to and including termination. Ensure 100% participation by stripping email and Web privileges from any employee who fails to complete training. Repeat the training and certification process annually as part of your annual review of Acceptable Usage Policies. ***Source:*** *"2006 Workplace E-Mail, Instant Messaging & Blog Survey" from American Management Association and The ePolicy Institute.*

3. Enforce Policy. Many employers find that the best way to manage people problems is through the application of technology solutions. If you have any doubt about your employees' willingness to adhere to email and Web usage and content rules, visit MessageLabs, www.messagelabs.com, to review policy-based management and monitoring technology solutions designed to help maximize employee compliance while minimizing workplace risks.

Don't allow employees to dismiss Acceptable Usage Policies as insignificant or unenforceable.

ePolicy Tip: Don't allow employees to dismiss Acceptable Usage Policies as insignificant or unenforceable. Take the lead from employers who increasingly are "putting teeth" in ePolicies. In the US, 26% of bosses have fired Internet abusers, and another 26% have dismissed email violators. Don't leave policy enforcement—and legitimate disciplinary action—to chance. Establish clear policy, educate all employees, and maximize compliance with policy-based monitoring and management technology tools. ***Sources:*** *2005 Electronic Monitoring & Surveillance Survey and 2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association and The ePolicy Institute*.

Ban Inappropriate Web Sites to Preserve Resources and Productivity

Use written Acceptable Usage Policies to alert 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 visiting online dating sites, 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 tools, www.messagelabs.com, designed to review and restrict inappropriate online behavior.

Email messages and Internet history create the electronic equivalent of DNA evidence... Take advantage of laws and management technology tools to help keep online employees in line.

ePolicy Tip: Email messages and Internet history create the electronic equivalent of DNA evidence. Fully 24% of employers have had employee e-mail subpoenaed by a court or regulator, and another 15% have gone to court to battle workplace lawsuits triggered by employee email. Don't allow email misuse and Web abuse sink your corporate ship. Take advantage of laws and management technology tools to help keep online employees in line. Thanks to the federal Electronic Communications Privacy Act, US employers have the right to monitor Web surfing and email transmissions. Fully 76% of bosses automatically track Web connections; 65% use technology to block access to inappropriate sites; and another 55% take advantage of management technology tools to record and review email. ***Sources:*** *2006 Workplace E-Mail, Instant Messaging & Blog Survey and 2005 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute*.

Control Email Risk by Controlling Written Content

Good email is businesslike and free of obscene, pornographic, sexual, harassing, menacing, defamatory, threatening, or otherwise offensive language and content. Good email is well-written and adheres to the rules of netiquette, or electronic etiquette. Reduce email risks by incorporating content rules that govern text, art, photos, cartoons, and other graphics into your email policy. Don't forget to ban jokes, gossip, rumors, innuendoes, and disparaging remarks that can lead to misunderstandings, hurt feelings, and legal claims. Many employers find content is best managed by policy-based management technology tools that monitor and filter messages that violate written policy, while protecting the system from spam, viruses, Trojan horses, worms, spyware, hackers, and other malicious intruders. Visit www.messagelabs.com for more information.

Top 10 Best Practices to Maximize Compliance and Minimize Email &Web Risk

Put Acceptable Usage Policies In Writing. Don't rely on email or the Intranet alone to inform employees of email and Web policies and procedures. Distribute a hard copy of each policy to every employee. Require employees to sign and date each policy, acknowledging they have read it, understand it, and agree to comply with it or accept the consequences, up to and including termination.

Educate Employees About Risks, Policies, and Compliance. Don't assume employees understand email and Web risks, and don't expect untrained employees to comply with Acceptable Usage Policies. The courts appreciate best practices-based policies that are supported by mandatory companywide training and backed by a combination of disciplinary action and management technology.

Establish Email Business Record Retention Guidelines. Should you ever face a workplace lawsuit, email business records will be subpoenaed **as** evidence. Nonetheless, 43% of business users report that they do not know the difference between business-critical email that must be retained and nonessential messages that can be purged from the system. As part of your strategic email management and Acceptable Usage Policy program, be sure to define "email business record" for your organization. Based on that definition, consistently apply formal retention rules, policies, procedures, and schedules to business-related/business record email.

Set Rules for Personal Use. Use Acceptable Usage Policies to spell out exactly how much personal email use and Web surfing is allowed, when, with whom, and under what circumstances. Be clear. Use specific language to prevent misunderstandings or individual interpretation of policy.

Recap Harassment, Discrimination, Ethics, Confidentiality, Security, and Other Policies. Company policy is company policy, regardless of the communications tool employed. Make sure employees understand that all company policies—including but not limited to those governing harassment, discrimination, ethics, confidentiality, and security—apply to email and Web use and content.

Stress Compliance with Sexual Harassment Policy. Because of the relaxed, informal nature of email, some employees will write comments they would never say aloud. Make sure employees understand that, regardless of how it is transmitted, an inappropriate comment is an inappropriate comment. All it takes is one off-color joke, "naughty" photo, sexually charged cartoon, or otherwise offensive message to trigger an expensive, protracted legal claim alleging a hostile work environment.

Address Monitoring and Privacy. Use clearly written, comprehensive Acceptable Usage Policies to notify employees—in clear and specific detail—of the organization's monitoring policies and practices. While only two states (Delaware and Connecticut) require employers to notify employees that they are being monitored, 89% of bosses alert workers that their Web usage is being tracked, and another 86% notify email users that they are being monitored, according to American Management Association/ePolicy Institute research.

Enforce Content Rules. Communicate the fact that email and the Web are to be used primarily as business communications tools. Clearly define approved and banned language and content. Insist that employees behave professionally and adhere to the rules of civil business behavior, also known as "netiquette" or electronic etiquette, when using the organization's email and Internet systems.

Support Acceptable Usage Policies with Technology. Because accidents happen (and disgruntled employees occasionally trigger intentional disasters), it's impossible to ensure 100% compliance. Support written rules with policy-based management technology tools, www.messagelabs.com, designed to monitor and filter content, block access to inappropriate sites, lock out malicious intruders, and retain and archive all-important email business records.

Don't Allow Employees to Dismiss Policy as Unenforceable. Make sure employees understand that their computer activity may be monitored. Stress the fact that policy violators will face disciplinary action that may include termination. Let employees know you mean business by enforcing your email and Web Acceptable Usage Policies consistently among all employees, regardless of rank or title.

> **ePolicy "Bonus" Tip:** 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 policies address every potential risk facing your organization and industry. Be certain policies and procedures 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. Your up-front investment in a 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.

Sample Web Acceptable Usage Policy

The Company is pleased to offer associates access to the organization's computer Network and the Internet. This Policy applies to employees granted Network and Internet access by the Company. For the Company to continue making Network and Internet access available, employees must behave appropriately and lawfully. Upon acceptance of your account information and agreement to follow this Policy, you will be granted Network and Internet access in your office. If you have any questions about the provisions of this Policy, you should contact the Chief Information Officer.

If you or anyone you allow to access your account (itself a violation of this Policy) violates this Policy, your access will be denied or withdrawn. In addition, you may be subject to disciplinary action, up to and including termination.

1. Personal Responsibility

> By accepting your account password and related information, and accessing the Company's Network or Internet system, you agree to adhere to this Policy. You also agree to report any Network or Internet misuse to the Chief Information Officer. Misuse includes Policy violations that harm another person or another individual's property.

2. Term of Permitted Use

> Network and Internet access extends throughout the term of your employment, provided you do not violate the organization's Computer Network and Internet Acceptable Usage Policy. Note: The Company may suspend access at any time for technical reasons, Policy violations, or other concerns.

3. Purpose and Use

> The Company offers access to its Network and Internet system for business purposes only. If you are unsure whether an activity constitutes appropriate business use, consult the Chief Information Officer.

4. Netiquette Rules

Employees must adhere to the rules of Network etiquette, or Netiquette. In other words, you must be polite, comply with the Company's ethics policy and code of conduct, adhere to the organization's electronic writing and content guidelines, and use the Network and Internet appropriately and legally. The Company will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

5. Banned Activity

The following activities violate the Company's Computer Network and Internet Acceptable Usage Policy:

(A) Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.

(B) Revealing personal information, such as the home address, telephone number, or financial data of another person or yourself.

(C) Making ethnic, sexual-preference, or gender-related slurs or jokes.

(D) Engaging in illegal activities, violating the Employee Handbook, or encouraging others to do so. Examples:

1. Selling or providing substances prohibited by the Company's employment policy or the Employee Handbook.

2. Accessing, transmitting, receiving, or seeking unauthorized, confidential information about clients or colleagues.

3. Conducting unauthorized business.

4. Viewing, transmitting, downloading, or searching for obscene, pornographic, or illegal materials.

5. Accessing others' folders, files, work, networks, or computers. Intercepting communications intended for others.

6. Downloading or transmitting the organization's confidential information or trade secrets.

(E) Causing harm or damaging others' property. Examples:

1. Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not marked with the copyright symbol, ©, employees should assume all materials are protected under copyright laws—unless explicit permission to use the materials is granted.

2. Using another employee's password to trick recipients into believing someone other than you is communicating or accessing the Network or Internet.

3. Uploading a virus, harmful component, or corrupted data. Vandalizing the Network.

4. Using software that is not licensed or approved by the Company.

(F) Jeopardizing the security of access, the Network, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.

(G) Accessing or attempting to access controversial or offensive materials. Network and Internet access may expose employees to illegal, defamatory, inaccurate, or offensive materials. Employees must avoid these sites. If you know of employees who are visiting offensive or harmful sites, report that use to the Company's Chief Information Officer.

(H) Engaging in commercial activity. Employees may not sell or buy anything over the Internet. Employees may not solicit or advertise the sale of any goods or services. Employees may not divulge private information—including credit card numbers and Social Security numbers—about themselves or others.

(I) Wasting the Company's computer resources. Specifically, do not waste printer toner or paper. Do not send electronic chain letters. Do not send email copies to nonessential readers. Do not send email to group lists unless it is appropriate for everyone on a list to receive the email. Do not send organization-wide emails without your supervisor's permission.

(J) Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content.

6. Confidential Information

Employees may have access to confidential information about the Company, our employees, and clients. With the approval of management, employees may use email to communicate confidential information internally to those with a need to know. Such email must be marked "Confidential." When in doubt, do not use email to communicate confidential material. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

7. Privacy

Network and Internet access is provided as a tool for our organization's business. The computer system is the property of the Company. The Company has the legal right to monitor usage of the Network and the Internet. Employees have no reasonable expectation of privacy when using the Company's computer system, Network, or Internet.

8. Noncompliance

Your use of the Network and the Internet is a privilege, not a right. Violate this policy and, at minimum, your access to the Network and the Internet will be terminated, perhaps for the duration of your tenure with the Company. Policy breaches include violating the above provisions, and failing to report violations by other users. Permitting another person to use your account or password to access the Network or the Internet—including but not limited to someone whose access has been denied or terminated—is a violation of Policy. Should another user violate this Policy while using your account, you will be held responsible, and both of you will be subject to disciplinary action.

Employee Acknowledgment

Note: If you have questions or concerns about this ePolicy, contact the Company's Chief Information Officer before signing this agreement.

I have read the Company's Computer Network and Internet Acceptable Usage Policy and agree to abide by it. I understand violation of any of the above terms may result in discipline, up to and including my termination.

_____	_____	_____
Employee Name (Printed)	Employee Signature	Date

Sample Email Acceptable Usage Policy

The Company provides employees with electronic communications tools, including an Email System. This written Email Acceptable Usage Policy, which governs employees' use of the Company's email system, applies to email use at the Company's headquarters and district offices, as well as at remote locations, including but not limited to employees' homes, airports, hotels, client and supplier offices. The Company's email rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates the Company's email rules and policies is subject to disciplinary action, up to and including termination.

Email Exists for Business Purposes.

The Company allows email access primarily for business purposes. Employees may use the Company's email system for personal use only in accordance with this policy. Employees are prohibited from using personal email software (Hotmail, etc.) for business or personal communications at the office.

Authorized Personal Use of Email

Employees may use email to communicate with spouses, children, domestic partners, and other family members. Employees' personal use of email is limited to lunch breaks and work breaks only. Employees may not use email during otherwise productive business hours.

Employees are prohibited from using email 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 a religious or other personal cause.

Privacy

The email system is the property of the Company. The Company has the legal right to monitor usage of the email system. Employees have no reasonable expectation of privacy when using the Company's email system.

Offensive Content and Harassing or Discriminatory Activities Are Banned

Employees are prohibited from using email 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 email 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 Company, negatively impact employee productivity, or harm employee morale.

Confidential, Proprietary, and Personal Information Must Be Protected

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

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

Business Record Retention

Email messages create written business records, and are subject to the Company's written and consistently applied rules and policies for retaining and deleting business records. See the Company's electronic business record retention policy for more information.

Violations

These guidelines are intended to provide Company employees with general examples of acceptable and unacceptable use of the Company'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 policies and procedures, address them to the Compliance 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 policies and procedures may result in disciplinary action, up to and including my termination.

_____
User Name

_____
User Signature

_____
Date

The ePolicy Institute

www.epolicyinstitute.com

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

The ePolicy Institute is dedicated to helping employers limit electronic risks, including litigation, through the development and implementation of Acceptable Usage Policies and employee training programs. An international speaker and trainer, Executive Director Nancy Flynn is the author of 8 books published in 4 languages. As a recognized authority on workplace Email and Web usage, Nancy Flynn is a popular media source who has been interviewed by *Fortune*, *Time*, *Financial Times*, *The Wall Street Journal*, *US News & World Report*, *Business Week*, *USA Today*, *New York Times*, National Public Radio, CNBC, CNN, CBS, ABC, and Fox News among others. ***Ten Easy Steps for Email & Web Best Practices*** is based on material excerpted from author Nancy Flynn's books *E-Mail Rules*, *Blog Rules*, *Instant Messaging Rules*, *The ePolicy Handbook*, *Writing Effective E-Mail*, and *E-Mail Management*.

MessageLabs

www.messagelabs.com

MessageLabs®

MessageLabs is the world's leading provider of messaging security and management services with more than 13,000 clients and offices in eight countries. For more information, please visit www.messagelabs.com.