

eMail Policy Guide
Best Practices for Clean and Compliant, Safe and Secure Workplace E-Mail

Nancy Flynn,
Executive Director, The ePolicy Institute
Author, *The ePolicy Handbook, Writing Effective E-Mail, E-Mail Rules*

© 2003, Nancy Flynn, The ePolicy Institute. All rights reserved.



CLEARSWIFT™

Managing and securing
electronic communications

Preface

The ePolicy Institute™, www.epolicyinstitute.com, and Clearswift, www.Clearswift.com, have created this book to provide guidelines for developing and implementing effective e-mail usage policies—and in the process creating safe and secure e-mail unlikely to trigger either a workplace lawsuit, employee termination or other electronic disaster.

The ePolicy Institute/Clearswift *eMail Policy Guide: Best Practices for Clean and Compliant, Safe and Secure Workplace E-Mail* is produced with the understanding that neither the author (Nancy Flynn, executive director of The ePolicy Institute), nor our Partner Clearswift is engaged in rendering legal, human resources, electronic risk management, or other professional services or advice. You should obtain legal counsel, human resources assistance, electronic risk management advice, and/or other expert assistance as required from competent professionals.

The eMail Policy Guide: Best Practices for Clean and Compliant, Safe and Secure Workplace E-Mail is based on material excerpted from author Nancy Flynn's book **The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies**, published by the American Management Association's Amacom publishing division, 2001. Called the most "useful business book this year, or next" by Training magazine, The ePolicy Handbook has been featured by The Wall Street Journal, US News & World Report, Kiplinger's Personal Finance, USAtoday.com, and thousands of international and national print, broadcast and online media outlets.

The ePolicy Institute is the leading source of information and tools about workplace e-risks, e-policies and e-mail. The Columbus, Ohio-based ePolicy Institute is dedicated to helping employers limit electronic liabilities while enhancing employees' eCommunications skills. In addition to selling books, content and training tools, The ePolicy Institute operates a speakers bureau and conducts training seminars for corporate and institutional clients across North America and around the globe. Visit www.epolicyinstitute.com to learn more about our products and services.

Clearswift is the world's leading provider of software for managing and securing electronic communications, with a 23% share of the global content filtering market. Clearswift delivers the capabilities for organizations to protect themselves against e-mail and web-based threats, meet legal and regulatory requirements, implement productivity-saving policies and manage intellectual property passing through their network. The company's expertise lies in establishing and enforcing e-policies. Content security threats include the circulation of inappropriate images and text, Spam and oversized files, loss and corruption of data, breaches of confidentiality, as well as viruses and malicious code. Clearswift's software portfolio includes Clearswift MIMESweeper, a product family for e-mail and web e-policies and Clearswift ENTERPRISEsuite, a software infrastructure for managing e-policies in complex environments. More information about Clearswift, its products and services is available at www.clearswift.com

© 2003, Nancy Flynn, The ePolicy Institute. All rights reserved. This publication may not be reproduced, stored in a retrieval system or transmitted in whole or in part, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of The ePolicy Institute, www.epolicyinstitute.com, 2300 Walhaven Ct., Suite 100A, Columbus, OH 43220. Phone 614/451-3200. E-mail experts@epolicyinstitute.com.

Why Every Organization Needs a Written E-Mail Policy

Whether you employ one part-time worker or 10,000 full-time professionals, if you allow employees access to your organization's e-mail system, you are putting your company's assets and future at risk.

In 2001, an estimated 1.4 trillion e-mail messages were sent from North American businesses, up from 40 billion in 1995, according to research firm International Data Corp. That level of electronic activity makes e-mail the most common—and potentially costly—form of business communication.

Think Your Employees Use E-Mail for Business Only? Think Again!

The facts, according to the **2003 E-Mail Rules, Policies and Practices Survey from American Management Association, The ePolicy Institute, and Clearswift:**

- 75% of organizations have e-mail policies in place.
- Only 48% of employers educate employees about e-mail risks, policy, and compliance.
- Merely 34% of employers have e-mail retention/deletion policies in place.
- Fully 22% of employers have fired employees for violating e-mail policy.
- 90% of organizations monitor incoming and outgoing e-mail.
- Only 19% of employers monitor internal e-mail among employees.

In the Electronic Office, Risks Abound

The most common and potentially costly electronic risks facing employers, according to the **2003 E-Mail Rules, Policies and Practices Survey from American Management Association, The ePolicy Institute, and Clearswift:**

- Workplace Lawsuits. One in 20 organizations has battled a legal claim triggered by employee e-mail.
- Lost Productivity. Fully 90% of employees send and receive personal e-mail at work.
- eSecurity Breaches--Theft of Confidential Data
- eSabotage—Triggered by Disgruntled Employees and Vengeful Ex-Employees
- Annoying Hacker Attacks
- Malicious Cracker Attacks
- Wasted Computer Resources. Fully 92% of employees receive spam at work.
- Computer Viruses. Over a third of businesses have received viruses via e-mail.
- Business Interruption. 38% of computer systems have been disabled thanks to e-mail.
- Regulatory Fines. In 2002, five Wall Street brokerages were fined \$8.3 million for failing to retain e-mail properly.
- Public Relations Nightmares

ePolicy + Education + Enforcement = Increased Compliance, Reduced Liabilities

Savvy employers eager to avoid electronic liabilities should take a three-step approach to reducing—and in some cases preventing—e-disaster. Combine a written e-mail policy with content filtering software and an ongoing employee education program to help keep online employees in-line.

Workplace Lawsuits

According to the **2003 E-Mail Rules, Policies and Practices Survey from American Management Association, The ePolicy Institute, and Clearswift**, 14% of workplace e-mail is subpoenaed by courts. And 1 in 20 employers has fought a claim of sexual/racial harassment/discrimination based on employees' e-mail and Internet use.

In one high-profile case, Chevron Corp. in 1995 was ordered to pay female employees \$2.2 million to settle a sexual harassment lawsuit stemming from inappropriate e-mail circulated by male employees. In 2000, inappropriate employee e-mail contributed to American Home Products' decision to settle a class-action lawsuit for a record-breaking \$3.75 billion.

Reduce electronic liabilities by notifying employees in writing you will not tolerate the electronic sending, receiving or viewing of offensive material. Use your written e-mail policy to spell out exactly what employees may and may not say via the company's e-mail system.

Lost Productivity

The 2003 E-Mail Rules, Policies and Practices Survey from American Management Association, The ePolicy Institute, and Clearswift shows the average employee spends 25% of the workday on e-mail.

If your employees are drowning in e-mail, it's a sure bet they aren't getting their work done. Use your written e-mail policy to establish guidelines for personal e-mail use. Most employers opt for 1 of 3 approaches:

1. Ban personal e-mail use completely.
2. Allow a limited amount of personal e-mail, as long as it falls within established guidelines. (Be sure to spell out those guidelines in your written e-mail policy).
3. Allow personal e-mail use, but only after normal business hours.

Wasted Talent

According to the **2003 E-Mail Rules, Policies and Practices Survey from American Management Association, The ePolicy Institute, and Clearswift** 22% of employers have terminated employees for violating written e-mail policy. Give employees rules to work by with a written e-mail policy, complete with content and CyberLanguage guidelines.

Guard against wrongful termination lawsuits by requiring all employees to acknowledge—with a signature and date—they have read your e-mail policy, understand it, and agree to comply with it or face the consequences, up to and including termination.

Public Relations Nightmares

E-mail disasters can trigger media scrutiny and public embarrassment. Consider the Federal Communications Commission (FCC) employee who inadvertently e-mailed a dirty joke to 6,000 reporters and government officials on the agency's group list. One employee's electronic mistake resulted in negative publicity and national embarrassment for the FCC.

Security Breaches & eSabotage

CyberCrime is one of the Net's leading growth industries, with e-mail making it easy for eSabotuers and electronic thieves to steal confidential data. Studies show 1 in 10 employees has received confidential company information via e-mail. Fully 79% of employees admit to sharing confidential information with other companies via e-mail. Use written e-mail policy to outlaw the sharing of confidential company information with outsiders and unauthorized insiders, too.

Wasted Computer Resources

Lockheed Martin's e-mail system crashed for 6 hours after an employee sent 60,000 coworkers a personal e-mail with a request for an electronic receipt. The defense contractor, which posts 40 million e-mails monthly, lost hundreds of thousands of dollars thanks to this one employee's action and the resulting system crash. You may not send 480 million e-mails a year, but you no doubt have made a sizable investment in a computer system designed to enhance productivity and improve business communications. If employees make personal use of your computer assets, your return on business investment will be minimal at best.

The Best Advice: Take a Proactive Approach to Risk Prevention

Don't wait for e-disaster to strike. Develop and implement a written e-mail policy, and enforce your policy with software and training.

No workplace ever can be 100% safe from e-mail risks. But with a written e-policy, filtering software and employee education, employers take big strides toward reducing e-risks, increasing productivity, and protecting corporate assets.

Forming Your E-Policy Team

Whether you operate a large organization with a full-time staff of in-house experts, or a small business that relies on part-time help and the advice of paid consultants, you will want to form an e-policy team to oversee the development and implementation of your e-mail policy. For most organizations, the e-policy team will be made up of some or all of the following professionals.

Senior Company Official

With a white knight leading the charge, your e-policy team should have no trouble receiving funding and support to complete its assignment.

Research Consultant

You can't change e-mail behavior until you know exactly what your employees are up to online. A comprehensive internal audit conducted by a professional research consultant or an e-policy team member will give you the information you need to develop a strategic e-policy program.

Human Resources Manager

Involve your HR manager in all aspects of the e-policy program, from planning, through writing, to training and enforcing. Don't have an in-house HR manager? Make the executive responsible for hiring, disciplining and terminating employees part of your e-policy team.

Chief Information Officer (CIO)

Your CIO can help bridge the gap between people problems and technical solutions, identifying electronic risks and recommending the most effective software tools and techniques to manage those risks.

Legal Counsel

Do not implement your e-mail policy until it's been reviewed by an experienced employment law or CyberLaw expert. Be sure all federal and state laws and regulations are addressed and everyone's rights are protected.

E-Risk Management Consultant

Effective electronic risk management couples management techniques with software tools. An e-risk management consultant can help you develop risk management guidelines that structure and support your e-mail usage policy.

Computer Security Expert

Be sure to assess and address your organization's computer security concerns and capabilities. Computer security policies and procedures help prevent disaster by keeping malicious external hackers and internal saboteurs out of your system.

CyberInsurance Broker

Mitigate e-liabilities with a comprehensive CyberInsurance program. Consult with an experienced CyberInsurance broker to review your e-risks and discuss the protection e-insurance offers.

Training Specialist

Your written e-policies are only as good as your employees' willingness to adhere to them. Support initial e-policy training with continuing education tools and programs.

Writing Coach

One of the most effective ways to control e-risks is to control written content. As part of your overall e-mail policy, establish an electronic writing policy to keep employee e-mail clean, clear and compliant.

Public Relations Manager

In the event of an electronic disaster, your PR manager will be responsible for keeping employees, the media, customers and shareholders informed, while killing rumors. Hope for the best, but plan for the worst with a written e-crisis communications plan as part of your comprehensive e-mail policy .

Uncovering E-Mail Misuse and Abuse with an E-Mail Audit

An internal e-mail usage audit reveals how employees are using, misusing and perhaps abusing e-mail. It also provides insights into how managers and supervisors can more effectively monitor employee e-mail use. Your internal e-audit will enable you to draft the right e-mail policy, install the most appropriate software to help manage your usage policy, and develop an effective training program to educate and motivate employees to adhere to e-mail policy.

Keep Managers in the Loop

Managers and supervisors can provide valuable insights into your organization's e-mail risks and e-policy needs. Some issue you may want to explore with managers while drafting your e-audit questionnaire:

1. When it comes to employee e-mail, what are the biggest problems you see?
2. What questions do employees most often ask about e-mail?
3. What is the greatest electronic risk facing our organization?
4. What challenges will we face as we start to implement our written e-mail policy?
5. Do you anticipate employee resistance to our new e-mail policy?
6. Are you comfortable serving as an e-mail policy trainer and enforcer?
7. What questions do you have about our electronic risks and e-mail policy?

Generate Staff Support for Your E-Audit

Maximize employee participation in the audit process and ensure honest responses by guaranteeing anonymity. Draft a questionnaire designed to uncover information about employees' e-mail use and abuse, along with the organization's electronic risks. For example:

- Do employees use the organization's e-mail system for personal use? Why and to what extent?
- What's the level of e-mail overload in your office? On a given workday, how much time do employees spend reading and writing e-mail messages?
- How many e-mail messages do employees receive daily?
- Do your employees send/receive inappropriate e-mail messages at work? What type and under what circumstances?
- Have employees been disciplined for sending or receiving personal e-mail messages?
- How do employees handle spam?
- Have employees ever sent or received harassing, discriminatory, or otherwise offensive e-mail messages?
- Do employees take time to ensure e-mail is well written and free of grammar, punctuation, and spelling errors?
- Do employees understand the why's and how's of e-mail deletion?
- Are employees aware e-mail can be used as evidence in workplace lawsuits?
- Are employees aware management has the right to read employee e-mail and monitor Internet use?
- Do employees know computers and passwords are the property of the company?
- Do employees know the basics of password and computer workstation security?
- Are employees using home computers for business purposes?

Protect Your Assets with an Effective E-Risk Management Policy

1. Police Document Creation and Content

One of the most effective ways to reduce e-risks is to control e-mail content. Good e-mail is businesslike and free of obscene, harassing, defamatory, or otherwise offensive language. Good e-mail is well-written and free from mechanical errors and structural problems. Ensure your employees' electronic communication is as effective as possible by instituting and enforcing an electronic writing policy as part of your comprehensive e-policy. Guarantee appropriate content by incorporating CyberLanguage guidelines into your e-mail policy.

Sample Content Statement

Employees may not use ABC Corp's e-mail system, network, or Internet/Intranet access for offensive or harassing statements or language including disparagement of others based on their race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

2. Establish a Document Retention and Deletion Policy

One of the most important components of a successful e-risk management program is an electronic document retention policy, providing formal guidelines for naming, archiving, or purging electronic files.

The best advice: Consult e-mail retention and deletion experts (ePolicy, CyberLaw and software professionals) who can help you establish an e-mail retention policy detailing how to categorize files, where to store files, and when and how to destroy files. You may want to supplement your retention/deletion policy with a software solution, as well.

3. Force Employees to Empty Their Mailboxes

An empty mailbox is a safe mailbox. Clean out overstuffed employee mailboxes with a combination of education and automation.

1. Explain the organization's e-risks and e-mail deletion guidelines. Instruct employees not to hold onto old e-mail messages.
2. Explain how the manual delete folder works.
3. Exercise control centrally with sophisticated management software technology. Assign limited e-mail space on your file server and reduce the size of employee mailboxes.
4. Install software enabling your e-mail systems administrator to empty employees' delete folders automatically.
5. Tell employees that saving messages to the hard drive is a violation of the organization's e-policy. Stress the fact that in a workplace lawsuit all material on employees' hard drives would be subject to legal review.

4. Limit Liability by Enforcing Risk Management Policies

Rely on your e-policy team to ensure successful implementation of both your e-risk management policy and your comprehensive e-mail policy. An effective e-risk management program should combine technological tools with people skills. Utilize the e-risk management software at your disposal, then add a big dose of common sense to the mix.

5. Keep Your Password to Yourself

In many offices, computers are treated casually, making it relatively easy for malicious persons to break in and steal data or funds. Institute password policies to lock out intruders:

1. Change all passwords quarterly, sooner if terminations, layoffs or other disruptions occur.
2. Passwords are the property of the employer. Maintain an updated record of employee passwords. Don't get locked out of your own computer system.
3. Instruct employees to store passwords in secure locations, not in unlocked desk drawers or taped to computer monitors.
4. Ban the use of passwords that reflect personal information. Have employees create passwords combining numbers, punctuation marks, and upper- and lower- case letters.

6. Restrict Computer Access

Instruct employees to shut off computers if they plan to be away from their desks for more than an hour. If you prefer to automate, establish a password system at the workstation or Network level requiring passwords to re-enter unattended computers. Also authorize your CIO to restrict remote access to your computers.

7. Investigate Unusual Behavior

Take steps to stifle employee misbehavior:

1. Have your CIO conduct periodic reviews to ensure employees are not attaching unauthorized storage devices to their computers.
2. Look for clues. If an employee brings a large, removable drive to work, ask what's up. Oversized removable drives are used to download really large files. Ignore the obvious, and you may facilitate the theft of valuable company data by an employee who is going into business or joining a competitor.
3. Conduct routine audits. If random reviews uncover problems, such as inappropriate language or extensive personal use of the system, take action. Develop a stricter e-mail policy, install filtering and/or monitoring software, or discipline the offender(s).

8. Use Software to Catch Bad Electronic Behavior—and Manage Appropriate Behavior

As an employer, you are obligated to create a harassment-free, discrimination-free work environment. You must control sexual harassment. You must prohibit the on-the-job collection and distribution of pornography. And you must prevent the use of e-mail as a tool to create an intolerable work environment. Many employers find control is best achieved by monitoring and/or filtering employee e-mail and Internet transmissions.

Don't leave e-risk management to chance. Install software to review and report employee e-mail use.

Clearswift is the world's leading provider of software for managing and securing electronic communications, with a 23% share of the global content filtering market. Clearswift delivers the capabilities for organizations to protect themselves against e-mail and web-based threats, meet legal and regulatory requirements, implement productivity-saving policies and manage intellectual property passing through their network. The company's expertise lies in establishing and enforcing e-policies. Content security threats include the circulation of inappropriate images and text, Spam and oversize files, loss and corruption of data, breaches of confidentiality, as well as viruses and malicious code. Clearswift's software portfolio includes Clearswift MIMESweeper, a product family for e-mail and web e-policies and Clearswift ENTERPRISEsuite, a software infrastructure for managing e-policies in complex environments. More information about Clearswift, its products and services is available at www.clearswift.com

Take E-Action Now

The ePolicy Institute and Clearswift recommend employers act today to prevent potentially costly e-disaster tomorrow. Steps to effective e-risk management:

1. Marshal the combined expertise of your e-policy team, and get to work on the timely development of written e-mail usage policies. Visit www.epolicyinstitute.com for policy development tips and tools, including ePolicy Forms Kits, *The ePolicy Handbook*, *E-Mail Rules*, *Writing Effective E-Mail*, and other products and services.
2. Involve managers early in the planning process, rallying their support for your e-mail policy and securing their commitment to policy enforcement.
3. Conduct a comprehensive internal audit to assess your organization's electronic liabilities, employees' e-mail capabilities, and the current level of e-mail misuse and abuse.
4. Use your e-audit to shape a customized e-mail policy that meets your organization's specific needs and risks.
5. Review your organization's document retention needs and legal requirements with a CyberLaw expert. Incorporate electronic document retention/deletion guidelines in your e-mail policy.
6. Institute a comprehensive e-risk management program coupling internal and external computer security with a big dose of common sense.
7. Install content filtering software to help manage and enforce your e-mail usage policy. Visit www.clearswift.com for the latest in software technology.
8. Conduct ongoing training to educate employees about e-risks and motivate compliance with e-mail policy. The ePolicy Institute conducts training seminars for corporate and institutional clients across North America and around the globe. E-mail Executive Director Nancy Flynn nancy@epolicyinstitute.com to discuss your training needs.

The ePolicy Institute

www.epolicyinstitute.com

The ePolicy Institute is the leading source of information and tools about workplace e-risks, e-policies and e-mail. The Columbus, Ohio-based ePolicy Institute is dedicated to helping employers limit electronic liabilities while enhancing employees' eCommunications skills.

The ePolicy Institute operates a speakers bureau and conducts seminars for corporate and institutional clients across North America and around the globe. Visit www.epolicyinstitute.com to learn about our seminars, products and services.

The ***E-Mail Policy Guide: Best Practices for Clean and Compliant, Safe and Secure Workplace E-Mail*** is based on material excerpted from Author and ePolicy Institute Executive Director Nancy Flynn's book *The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies* (Amacom, 2001). Nancy Flynn is the author of several other books, including ***E-Mail Rules*** (Amacom 2003) and ***Writing Effective E-Mail*** (Crisp 2003, 1998), published in the United States, China, Germany and Spain.

Noted for her e-policy and e-mail expertise, ePolicy Institute Executive Director Nancy Flynn has been interviewed by *The Wall Street Journal*, *Fortune*, *New York Times*, *US News & World Report*, *Kiplinger's Personal Finance*, *USAtoday.com*, *HR Executive*, *Training*, *Woman's Day*, *Home Office Computing*, *Good Housekeeping*, *the Associated Press*, *the Los Angeles Times*, *Chicago Tribune*, *National Public Radio*, *CNN Headline News*, *CBS MarketWatch*, *the CBS Radio Network*, *the ABC Radio Network*, *CNN Online*, and *ABC Online* and thousands of international and national print, broadcast and online media outlets.