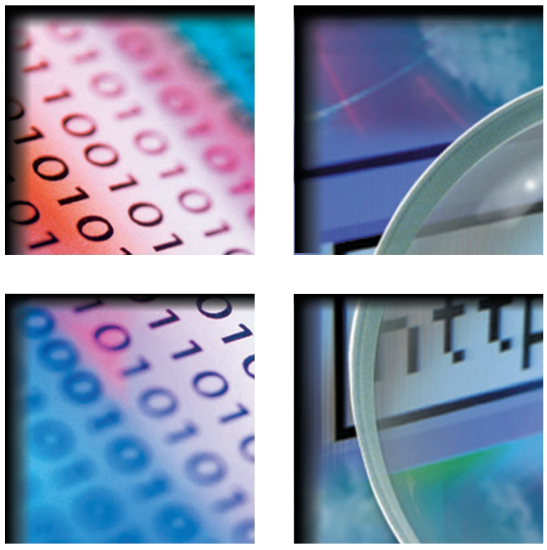
Internet Manager®
Web and Email Filtering Solutions

THE EPOLICY INSTITUTE™ / ELRON SOFTWARE, INC.

E-Mail Policy Guide

A Formula for Safe and Secure E-Mail Usage

- Find out why your organization should outline acceptable e-mail usage standards
- Learn how to conduct an e-mail audit and draft an effective e-mail policy
- Discover how e-mail content filtering solutions can help enforce your policy



ELRON SOFTWARE

E-Mail Policy Guide

A Formula for Safe and Secure E-Mail Usage

By Nancy Flynn

Executive Director, The ePolicy Institute

Author, *The ePolicy Handbook* and *Writing Effective E-Mail*

Elron Software, Inc.
7 New England Executive Park
Burlington, MA 01803
Tel: (781) 993-6000
Fax: (781) 993-6001
www.elronsoftware.com

The ePolicy Institute
Walhaven Ct., Suite 100A
Columbus, OH 43220
Tel: (614) 451-3200
E-mail: experts@epolicyinstitute.com
www.epolicyinstitute.com

epolicywp3/02DM 011-BKL-0068

Preface

The ePolicy Institute™, www.epolicyinstitute.com, and Elron Software, Inc., www.elronsoftware.com, have written this guide to provide helpful advice for developing and implementing effective e-mail usage policies—and, in the process, creating safe and secure e-mail unlikely to trigger a workplace lawsuit, employee termination or other electronic disasters.

The ePolicy Institute/Elron Software, Inc. ***E-Mail Policy Guide: A Formula for Safe and Secure E-Mail Usage*** is produced with the understanding that neither the author (Nancy Flynn, executive director of The ePolicy Institute) nor the publisher (Elron Software, Inc.) 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 guidance as required from competent professionals.

The ***E-Mail Policy Guide: A Formula for Safe and Secure E-Mail Usage*** 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.

Table of Contents

What You Don't Know Can Hurt You—Why Every Organization Needs a Written E-mail Policy 5

Step 1: Uncover Misuse and Abuse with an E-mail Audit 8

Step 2: Form an E-mail Policy Team 9

Step 3: Draft an Effective E-mail Policy 11

Step 4: Enforce Your E-mail Policy 14

Appendix A: E-mail Policy Guide Checklist 15

Appendix B: About The ePolicy Institute 16

Appendix C: About Elron Software, Inc. 16

What You Don't Know Can Hurt You—Why Every Organization Needs a Written E-mail Policy

Think your employees use e-mail for business purposes only? Think again! 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 International Data Corp. That level of electronic activity makes e-mail the most common—and potentially costly—form of business communication.

The facts, according to Elron Software's *1999 E-Mail Abuse Study*:

- 86% of employees send and receive personal e-mail at work.
- 60% of employees send or receive adult-oriented e-mail at work.
- 55% of employees send or receive politically incorrect or otherwise offensive e-mail at work.

IN THE ELECTRONIC OFFICE, RISKS ABOUND

The most common and potentially costly electronic risks facing employers:

- Workplace Lawsuits (sexual and racial harassment/discrimination, wrongful termination, hostile work environment, defamation, copyright infringement, invasion of privacy…the list goes on)
- Lost Productivity
- eSecurity Breaches—Theft of Confidential Data
- eSabotage—Triggered by Disgruntled Employees and Vengeful Ex-Employees
- Annoying Hacker Attacks
- Malicious Cracker Attacks
- Wasted Computer Resources
- Computer Viruses
- Business Interruption
- Fines & Imprisonment
- Public Relations Nightmares

Workplace Lawsuits

According to the *2001 ePolicy Survey* from the American Management Association (AMA), *US News & World Report* and The ePolicy Institute, 10% of Fortune 1000 companies' workplace e-mail has been subpoenaed by courts. And 11% of employers have fought claims of sexual/racial harassment/discrimination based on employees' e-mail and Internet use.

In one high-profile case in 1995, Chevron Corp. 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 that 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.

Wrongful Termination

According to the AMA, *US News & World Report*, ePolicy Institute *2001 ePolicy Survey*, 17% of employers have terminated employees for violating written e-mail and/or Internet policy. Give employees rules to work by. Develop 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.

Lost Productivity

Recent studies show employees spend anywhere from 49 minutes to 4 hours a day e-mailing. Adding to the problem, as reported in Elron Software's *2001 Corporate Web and Email Usage Study*, 30% of business e-mail users receive jokes and chain letters daily.

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.

eSecurity Breaches & eSabotage

CyberCrime is one of the Net's leading growth industries, with e-mail making it easy for eSaboteurs and electronic thieves to steal confidential data. Elron Software's *1999 E-Mail Abuse Study* reveals 1 in 10 employees has received confidential company information via e-mail. And, 79% of employees admit to sharing confidential information with other companies via e-mail. Use a written e-mail policy to prevent the sharing of confidential company information with outsiders and unauthorized insiders, too.

Wasted Computer Resources

Lockheed Martin's e-mail system crashed for six hours after an employee sent 60,000 co-workers 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.

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.

THE BEST ADVICE: TAKE A PROACTIVE APPROACH TO RISK PREVENTION

Don't wait for e-disaster to strike. 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.

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.

Step 1: Uncover 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-mail audit will enable you to draft the right e-mail policy, install the most appropriate software to help manage your policy, and develop an effective training program to educate and motivate employees to adhere to the 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 issues you may want to explore with managers while drafting your e-mail audit questionnaire include:

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

GENERATE STAFF SUPPORT FOR YOUR E-MAIL 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?
- 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?
- Do employees subscribe to e-newsletters or other electronic news services? What kind and how many?

Step 2: Form an E-mail 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. 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, 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 your organization's rights, as well as those of your employees, 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 squelching 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.

Step 3: Draft an Effective E-mail Policy

By allowing employees to access e-mail, employers have created one more avenue down which they can be dragged into litigation. The best protection available to employers is a comprehensive e-mail policy that defines what is and is not acceptable use of the organization's computer assets. If you think a brief, informal policy along the lines of, "The company's computer system is reserved for business use only," will protect you, think again. Regardless of the industry in which you operate or the size of your company, it is important to give employees consistently enforced rules for acceptable e-mail usage.

THINK BEFORE YOU SEND

E-mail may be one of the quickest and easiest ways to communicate, but that does not necessarily make it the most appropriate way to conduct business. Advise employees to think before they write. Assess each situation individually to determine whether the message is best communicated via e-mail, or if the telephone or a face-to-face meeting might be better!

Instruct Employees to Avoid E-mail When . . .

- A message is important or confidential and you can't risk a breach of privacy. E-mail simply isn't secure.
- You want to negotiate or hold a give-and-take conversation.
- You need detailed answers to a long list of questions.
- You need to deliver bad news.
- An immediate response is required.
- You need to confer with several people simultaneously.
- You risk offending the reader with a poorly worded message.
- There's a risk your message will be misunderstood.

Advise Employees to Use E-mail When . . .

- You want to deliver a message quickly and aren't concerned about reply speed.
- You want to communicate directly with decision-makers who read and respond to their own e-mail.
- You want to avoid phone, fax and delivery costs.
- You need to communicate with readers in other time zones or countries.
- You want to deliver one message to many readers.
- You need a written record of your conversation.
- You're on a tight deadline.
- You want to eliminate the costs and waste associated with hard copies.
- You want to stay in touch while traveling.

Guidelines for Personal E-mail Use

With regard to personal e-mail use during the workday, most employers opt for one of the following approaches:

- Ban personal e-mail use completely.
- 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.)
- Allow personal e-mail use, but only after normal business hours.

Attachment Guidelines for E-mail Senders

- Determine if your recipient's system can accommodate your attachment.
- Ask if your recipient's e-mail policy outlaws the opening of attachments.
- Attach first; write your message second.
- Write a brief yet compelling message to motivate the reader to open the attachment.
- Limit copies strictly to those with a genuine need to read your message and attachment.
- Never send an attachment if a brief message will do.
- Compress extremely large files.

Attachment Guidelines for E-mail Receivers

- If you don't know the sender, don't open the attachment.
- If the accompanying message is odd, don't open the attachment.
- If the subject line is questionable, delete the message without opening the attachment.

Forwarding E-mail

Use your e-mail policy to address the forwarding of messages. Ask permission from the original sender before forwarding a message. The message you forward could contain confidential or copyright-protected material.

Listserv Guidelines

Listservs can create overwhelming amounts of spam. Reduce the burden on your e-mail server and control employees' online time by establishing guidelines for listserv participation. Restrict employee subscriptions to authorized, business-related listservs.

Writing Guidelines

Just because e-mail gets there faster does not mean you should spend less time sweating the mechanical details. All business correspondence, whether electronic or traditional, projects an image of the individual writer and the organization as a whole.

An e-mail document full of errors will tax the reader's patience and lessen the writer's credibility. In the battle for the reader's on-screen attention, carefully written e-mail that is free of mechanical errors is sure to come out the winner.

SAMPLE POLICY

While brief is bad, you also want to avoid policies that are excessively long or intimidating. The best advice: Keep policies simple; keep policies straightforward, and make policies accessible. Below is a sample e-mail policy.

Employee E-mail Usage Policy

E-mail is to be used for ABC Company business and should not be overused or misused. Personal e-mail use is allowed before 8:30 a.m. and after 5:30 p.m. E-mail is an efficient way to send urgent messages or those designed to communicate with multiple people simultaneously. Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s).

ABC Company may access and monitor e-mail at any time for any reason without notice. You should not expect or treat e-mail as confidential or private. E-mail users must provide the network administrator with passwords. Except for authorized Company personnel, no one is permitted to access another person's e-mail without consent.

System users should exercise extreme judgment and common sense when distributing messages. Confidential information should never be disseminated to unauthorized sources. This includes the transmission of documents containing financial information or Social Security numbers. Client-related messages should be carefully guarded and protected, like any other written materials. You must also abide by copyright laws, ethics rules and other applicable laws.

Sending harassing, abusive, intimidating, discriminatory, or other offensive e-mails is strictly prohibited. The use of the system to solicit for any purpose without the consent of the human resources director is strictly prohibited. If you receive a message containing defamatory, obscene, offensive or harassing information, or that discloses personal information without permission, you must delete it immediately and not forward it. Chain-type messages and executable graphics files should also be deleted and not forwarded because they cause overload on our system. Anyone engaging in the transmission of inappropriate e-mails, as determined by the Company, will be subject to discipline, up to and including termination.

I have read the Company's e-mail policy and agree to abide by it as consideration for my continued employment. I understand that violation of any above policies may result in my termination.

_____ _____

User Signature Date

Source: © 2001, 2002, The ePolicy Institute, Executive Director Nancy Flynn.
For informational purposes only. No reliance should be placed on this without the advice of counsel.

MOVING FORWARD

Conduct routine e-mail 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 and/or discipline the offender(s).

Step 4: Enforce Your E-mail Policy

Use Software to Monitor and Manage Electronic Behavior

Policy without enforcement is useless. 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 installing software to monitor and/or filter employee e-mail and Internet transmissions. In addition, such software can protect employees from unwarranted accusations or terminations for Internet activity they did not engage in. To prevent errors, it is important to choose filtering software that can accurately track and report individual Internet use down to the minute.

Don't leave e-mail management to chance. Install software to monitor and report on employee e-mail use. Elron Software offers IM Message Inspector—an award-winning e-mail content filtering solution that proactively monitors, manages and, if necessary, blocks unauthorized inbound, outbound and interoffice electronic communications. Awarded *PC Magazine's* prestigious "Editor's Choice" for excellent content filtering and spam technologies, Message Inspector can enforce your unique e-mail policy with precision, flexibility and ease.

For more information, visit www.elronsoftware.com.

Appendix A: E-mail Policy Guide Checklist

The ePolicy Institute and Elron Software recommend employers act today to prevent a potentially costly e-disaster tomorrow. Steps to effective e-mail 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* 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. Your written policy should spell out clearly what is, and is not, allowed to be communicated via your organization's e-mail system.
6. Make the development and implementation of your e-mail policy a company-wide initiative. Review your policy with all employees, including full-time, part-time and temporary staff, as well as independent contractors and freelancers who work on behalf of your organization. Educate managers and supervisors about the importance of consistently enforcing the organization's e-mail policy.
7. Remember that writing a comprehensive e-mail policy is only half the battle. To win the war, you must install content filtering software to help manage and enforce your e-mail usage policy. Visit www.elronsoftware.com for the latest information on filtering technology.
8. Conduct ongoing training to educate employees about e-risks and motivate compliance with your e-mail policy.

Appendix B: About 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: A Formula for Safe and Secure E-Mail Usage*** 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 *Writing Effective E-Mail* (Crisp, 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, 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, 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.

Appendix C: About Elron Software, Inc.

www.elronsoftware.com

Elron Software's Internet Manager product family, including IM Web Inspector™, IM Message Inspector™ and IM Anti-Virus™, is a comprehensive set of solutions for web access control, e-mail content filtering and virus protection. These award-winning security solutions maximize the productive use of the Internet while minimizing the associated risks: confidential data loss, reduced productivity, legal liability, network congestion and virus attacks. With worldwide headquarters in Burlington, Massachusetts, Elron Software is a private company whose investors include Elron Electronic Industries (Nasdaq: ELRN) and Critical Path (Nasdaq:CPTH). For more information, please visit www.elronsoftware.com or call 800-767-6683.

Elron Software, Inc. · 7 New England Executive Park · Burlington, MA 01803 · Tel: (781) 993-6000 · Fax: (781) 993-6001