



**presents**

## **Top Tips for E-Mail Management**

***Best Practices to Successfully Manage E-Mail to Maximize Compliance and Minimize Risk***

*By*

Nancy Flynn

Executive Director, The ePolicy Institute

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

© 2007 Nancy Flynn, The ePolicy Institute. All rights reserved.

**TABLE OF CONTENTS**

**Preface** ..... **3**

**E-Mail Rule #1:** Treat E-Mail as a Business Record..... **4**

**E-Mail Rule #2:** Understand Federal Rules of Civil Procedure..... **5**

**E-Mail Rule #3:** Determine What You Need—or Want—to Retain  
as a Business Record ..... **6**

**E-Mail Rule #4:** Adhere to Regulatory Rules Governing Business  
Records..... **6**

**E-Mail Rule #5:** Use Registered E-mail to Protect Your  
Company from Deliberate Fraud and False Claims—and Create  
Legally Valid Evidence of Transmissions..... **9**

**E-Mail Rule #6:** Apply the 3-E’s of Strategic Electronic  
Communication Management ..... **11**

**Best Practices Review:** Do’s & Don’ts for Strategic E-Mail  
Management..... **13**

**Sample E-Mail Policy**..... **16**

**The ePolicy Institute** ..... **19**

## Preface

The ePolicy Institute™, [www.epolicyinstitute.com](http://www.epolicyinstitute.com) and RPost®, the provider of Registered E-mail® services, [www.rpost.com](http://www.rpost.com), have created this business Toolkit to provide best-practices-based guidelines for the strategic and effective management of workplace e-mail and electronic business records.

Through the implementation of: (1) Clearly written rules and policies governing e-mail usage, content and retention; (2) Comprehensive employee training programs to ensure that employees can distinguish business record e-mail from non-record communication; and (3) Technology tools designed to retain/archive e-mail business records in a legally sound manner—employers can maximize compliance while minimizing the likelihood and/or expense of litigation, regulatory investigations, compromised confidences, and other electronic communication disasters.

The ePolicy Institute/RPost Toolkit, ***Top Tips for E-Mail Management: Best Practices to Successfully Manage E-Mail to Maximize Compliance and Minimize Risk***, is produced as a general best-practices guide with the understanding that the author and publisher, Nancy Flynn, Executive Director of The ePolicy Institute, is not engaged in rendering advice on legal, regulatory, compliance, or other issues. Before acting on any issue, rule, best practice, or policy addressed in ***Top Tips for E-Mail Management***, you should consult with legal counsel or other professionals competent to review the relevant issue.

***Top Tips for E-Mail Management*** is based on material excerpted from author Nancy Flynn's books *E-Mail Management*, *E-Mail Rules*, *Instant Messaging Rules*, *Blog Rules*, *The ePolicy Handbook*, and *Writing Effective E-Mail*.

**The ePolicy Institute** is a leading source of speaking, training, and consulting services related to workplace E-mail/IM/Web/Blog risks, policies, and management. The ePolicy Institute is dedicated to helping employers limit e-mail/IM and Web/blog risks, including litigation and regulatory investigations, while enhancing employees' electronic communication skills. Visit [www.epolicyinstitute.com](http://www.epolicyinstitute.com) to learn more.

© 2007 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 Author and Executive Director Nancy Flynn, The ePolicy Institute, [www.epolicyinstitute.com](http://www.epolicyinstitute.com), 2300 Walhaven Ct., Columbus, OH, USA 43220. Phone 614/451-3200. Contact Nancy Flynn via e-mail: [nancy@epolicyinstitute.com](mailto:nancy@epolicyinstitute.com).

## E-Mail Rule #1: Treat E-Mail as a Business Record

**E-mail messages create the electronic equivalent of DNA evidence. Fully 24% of employers have had e-mail subpoenaed by courts and regulators; another 15% have battled lawsuits triggered by employee e-mail.**

*Source: American Management Association/ePolicy Institute 2006 Workplace E-Mail, Instant Messaging, Blog Survey.)*

From a legal perspective, the process of formally defining, properly identifying, and effectively retaining business records is one of the most important e-mail management activities your organization can engage in. Your ability to separate e-mail business records (business-critical e-mail) from insignificant non-record messages can have an enormous impact on your organization's business assets, reputation, and future should you one day find yourself battling a workplace lawsuit or regulatory investigation.

Heightened regulatory oversight and a highly litigious business environment bring new and potentially costly challenges to corporate e-mail systems. The business community's failure to properly manage e-mail business records and other forms of electronically stored information is alarming.

**Only 57% of employees know the difference between an electronic business record that must be retained and a non-record that may be purged. Merely 34% of employers have an e-mail retention policy in place.**

*Source: 2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association and The ePolicy Institute.*

The accidental misuse (and intentional abuse) of e-mail by employees and malicious third-parties can create expensive and time-consuming legal, regulatory, security, and productivity headaches for employers. High-profile e-mail gaffes have triggered everything from tumbling stock prices to seven-figure legal settlements to billion-dollar regulatory fines to media feeding frenzies.

Regardless of your organization's industry, size, or status as a public or private entity, the most effective way to prevent e-mail-related disasters—including costly and protracted lawsuits, regulatory investigations and fines, and the loss of confidential information—is to develop and enforce a strategic e-mail management program that addresses usage, content authentication, and record retention / retrieval capabilities among other key issues.

## E-Mail Rule #2: Understand Federal Rules of Civil Procedure

On December 1, 2006, the United States Federal Court announced amended rules governing the discovery of "*Electronically Stored Information*" (ESI). A newly minted phrase, *Electronically Stored Information* refers to e-mail and any other type of data that can be stored electronically. ESI is intended by the Court to be broad enough to cover all current types of computer-based information, yet flexible enough to accommodate future changes and technology developments.

### The Federal Rules of Civil Procedure make clear the following:

1. Electronically stored information (ESI) is discoverable and may be used as evidence—for or against your company—in litigation.
2. Business record ESI (related to litigation) must be retained, archived, and produced during discovery, which is the evidence-gathering phase of litigation.
3. Companies are allowed to routinely purge archives of data not relevant to litigation or pending cases.
4. Writing over backup tape may constitute *virtual shredding* once litigation is underway.
5. To be accepted as evidence, e-mail must be trustworthy, authentic and tamperproof.

A whopping 83% of business data resides in e-mail, according to industry estimates. All that ESI can trigger financial, productivity, and legal nightmares—should your organization find itself embroiled in a workplace lawsuit. The cost and time required to produce subpoenaed e-mail, retain legal counsel, secure expert witnesses, mount a legal battle, and cover jury awards and settlements—could put you out of business.

**"Any form of documentary evidence can be altered. But, it takes some skill to forge a paper signature; however, altering an e-mail takes nothing more than an impure heart and a keystroke."**

—Maryland Chief Magistrate Judge Paul Grimm, *Lorraine v. Markle American Insurance Co.*

To be considered legally valid, e-mail must be deemed by the court to be authentic, trustworthy, and tamperproof. Unfortunately, standard e-mail can easily be

changed—just by clicking “edit” and “change.” Even all-important business records can easily be forged when they are sent or received via standard e-mail.

### **E-Mail Rule #3: Determine What You Need—or Want—to Retain as a Business Record**

A business record provides evidence of a company’s business-related activities, events, and transactions. Business records are retained according to their ongoing business, legal, compliance, operational, and historic value to the company.

Not every message that enters or leaves your e-mail system is a business record. Not every electronic conversation you conduct rises to the level of a business record. Your organization’s welfare depends on your ability to distinguish business records from insignificant non-record messages. When it comes to business records, best practices call for the following:

1. Establish a clear definition of “business record” on a companywide or department-by department basis.
2. Know—and adhere to—the courts’ and regulators’ ESI record retention and production rules.
3. Communicate the company’s “business record” definition clearly and consistently to all employees. Make sure employees know the difference between records and non-records—and understand their individual roles in the retention of records and the purging of non-records.
4. Establish written policies and schedules governing the retention and disposition of ESI records, as well as the purging of non-records.

### **E-Mail Rule #4: Adhere to Regulatory Rules Governing Business Records**

In the United States, organizations that have yet to adopt a strategic e-mail management program face regulatory challenges and legal risks including:

1. **Sarbanes-Oxley (SOX) Regulations:** For public companies and registered public accounting firms, inadequate e-mail management and lax e-mail security can lead to SOX violations. Designed by the Securities and Exchange Commission (SEC) to thwart fraud in public companies, SOX

requires regulated companies to implement internal controls for gathering, processing and reporting accurate and reliable financial information. In other words, SOX requires businesses to demonstrate effective corporate governance and information management controls.

Effective e-mail management is fundamental to SOX compliance. The most common means of business communication, e-mail is used to transmit financial information and related documents internally and externally. Consequently, e-mail security breaches, from intercepted messages to corrupted files to leaked, stolen or lost data, can put an organization at risk of non-compliance. When it comes to e-mail security, regulated and non-regulated companies alike have reason for concern. According to the annual CSI/FBI Computer Crime and Security Survey, 56% of organizations reported unauthorized use of their computer systems in 2005, up from 53% the previous year. Dollar losses from unauthorized access to information increased nearly six-fold per respondent between 2004 - 2005, with average per-respondent losses from the theft of proprietary information nearly doubling.

Just how tough is the SEC on SOX violators? Failure to retain e-mail related to audit work papers and financial controls for at least seven years as mandated by SOX can put your organization at risk of severe penalties for non-compliance. Knowingly altering or destroying records that are vital to an audit or investigation can net guilty parties 20 years in federal prison. While SOX is vague about e-mail requirements and electronic record keeping, employers are advised to implement an e-mail management program that addresses usage, content, security and retention as part of the organization's comprehensive SOX compliance plan.

- 2. SOX and Private Companies:** While not regulated by SOX, private companies are coming under increasing pressure to comply with SOX provisions that have been recognized as industry best practices. According to the 2005 CSI/FBI Computer Crime and Security Survey, respondents in eight out of 14 regulated and non-regulated industries including utility, high-tech, manufacturing, medical, telecommunications, educational, financial, transportation, state government, retail, legal, local government, and federal government believe that SOX has an impact on their organizations' information security. In contrast, respondents from only five of these 14 industry categories reported an impact from SOX in 2004.

From lenders and insurers, to prospective merger partners, to disgruntled shareholders and other potential litigants, to federal regulators and government entities, private companies can satisfy a broad range of

audiences by taking the SOX approach to financial oversight. Private companies eager to comply with SOX should review their e-mail management, policy and content security programs to ensure that financial data and related documents—including for example confidential internal memos, revenue projections or other content transmitted via e-mail, are effectively managed, properly retained, safe from digital attacks, and otherwise SOX compliant.

3. **Health Insurance Portability and Accountability Act (HIPAA):** Companies in the health care industry are legally required by the Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy of patient information. HIPAA requires healthcare organizations to safeguard e-mail 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. Organizations that are governed by HIPAA have a choice: either use policy, training and technology, including content security and encryption software, to ensure the safe and compliant use of e-mail to transmit and store HIPAA-regulated patient information, or suffer potentially stiff penalties for noncompliance.
4. **Gramm-Leach-Bliley Act (GLBA):** GLBA is to the financial industry what HIPAA is to the health care arena. Under GLBA, financial institutions are legally obligated to protect the privacy of customers and their nonpublic personal information. In spite of Congress' attempts to protect customer privacy and regulate corporate accountability, many organizations remain challenged by GLBA, along with other federal and state regulations. Employee education is key to regulatory compliance. A company cannot expect untrained employees to be familiar with rules and regulations, appreciate the importance of compliance, or understand their individual roles in the compliance process. Support written e-mail policy with training and stress the fact that regulatory compliance is not an option, it is mandatory.
5. **SEC and NASD Rules and Regulations:** Broker-dealers and other regulated financial services firms that fail to manage written e-mail content or retain e-mail business records according to SEC and National Association of Securities Dealers (NASD) regulations, can face lengthy investigations, seven-figure fines and embarrassing headlines. For example, in February 2005, the SEC reached a \$2.1 million settlement with J.P. Morgan Securities for its failure to retain company e-mail. In 2003, the SEC fined six Wall Street brokerage firms a combined \$1.4 billion for failing to retain e-mail according to SEC guidelines. Any company regulated by the SEC or NASD

that has yet to adopt e-mail best practices based on regulatory rules should be prepared for equally robust penalties.

- 6. NYSE Regulations:** Like SEC and NASD-regulated firms, companies that are listed on the New York Stock Exchange must manage e-mail according to NYSE content and retention guidelines. They also are required to protect confidential business information and customers' personal data. Since much company and customer data is stored on computers and transmitted via e-mail, it is essential for NYSE-listed companies to put policies, procedures and content security technology in place to protect confidential information from e-mail security breaches and other computer-related disasters.

When it comes to e-mail management and e-mail business record retention, the courts and regulators take compliance seriously. SOX, GLBA, HIPAA, NYSE, SEC and NASD aren't the only regulations and agencies that employers need to worry about. The Food and Drug Administration (FDA), Environmental Protection Agency (EPA), Internal Revenue Service (IRS), Occupational Safety and Health Administration (OSHA), state insurance regulators and other federal and state agencies regularly request access to e-mail for audit or review.

If unsure which government or industry regulations govern your industry and your employees' use of e-mail, now is the time to find out. Assign a team of legal, compliance, records management and IT professionals to determine where e-mail fits into your organization's regulatory puzzle, and how a program that combines written policy, employee education, and technology (the Three-Es of e-mail risk management) can help maximize compliance and minimize e-mail-related disasters.

## **E-Mail Rule #5: Use Registered E-mail to Protect Your Company from Deliberate Fraud and False Claims—and Create Legally Valid Evidence of Transmissions**

Fortunately, there is a way to protect your company from deliberate fraud and false claims including "I didn't get your e-mail," or "That's not the attachment I sent," or even worse "I got your e-mail but that is not what it said." RPost® Registered E-mail® services provide e-mail users with legally valid evidence of precisely what e-mail content and attachments were sent and received, by whom and when. The service closes the delivery gap in electronic communications that may result when unprotected important e-mail messages are disputed with respect to content or

delivery status. RPost Registered E-mail services provide a much-needed new safeguard for electronic business communications.

RPost® Registered E-mail® service is the only simple, cost-effective way to provide e-mailers the same verifiable protections associated with hard-copy documents, but without requiring the recipient to maintain passwords, keys or install software. The RPost Registered E-mail core service provides the sender with verifiable proof of sending and receiving; content (including attachments); and the atomic clock time stamps. The Registered Receipt™ e-mail (that is returned automatically to the sender) is the strength of the service in that it provides a digital recording / snapshot of the server-to-server conversation that witnessed the e-mail transaction. The same receipt is then used to regenerate the original e-mail and attachments should anyone challenge the original transaction after-the-fact. Therefore, the inherent records management aspect of the RPost Registered Receipt e-mail allows a company to archive important e-mail transactions without having an elaborate document retention system in place. A simple rule of thumb to keep in mind when sending business e-mail is – “if it is important enough to send the e-mail as a Registered E-mail message, it is important enough to archive. The Registered Receipt e-mail establishes the official record for safekeeping.”

When using the RPost Registered E-mail service, best practices dictate the following:

1. Work with your legal counsel to determine what a business record is and how e-mail business records are to be managed and archived.
2. Educate all employees, from the summer intern to the CEO, to ensure that everyone knows the difference between business record e-mail and non-records.
3. Educate employees on the use of Registered E-mail® service – “*if the e-mail commits the company to anything at all, send it Registered.*” Understand that having a “store everything” e-mail policy is not practical, as important electronic documents are not segregated from casual e-mail and employees are less conscious of protecting the company. Also, traditional archive systems record only what was sent and fall short of protecting the sender whose e-mail receipt and / or content and relevant times may be challenged subsequently by the recipient. An archive system that can retrieve a simple text copy of an e-mail that was sent, can still fall prey to the recipient’s likely accusation of non-receipt or a possible challenge of what the e-mail actually said and when in fact it was received.
4. Implement written rules and policies governing the use of Registered E-mail service.

5. Integrate your Registered E-mail service rules and policies into your organization's comprehensive strategic electronic communication program.
6. Establish a master back-up archive system for all Registered Receipt e-mails as those left on employees' desktops can be inadvertently deleted. Because RPost does not store any information, it is incapable of providing replacement Registered Receipt e-mail.

## E-Mail Rule #6: Apply the 3-E's of Strategic Electronic Communication Management

Put best practices to work by focusing on the 3-Es of Strategic Electronic Communication Management: (1) Establish policies; (2) Educate employees; and (3) Enforce policies with disciplinary action and technology tools.

1. **Establish** comprehensive, clearly written rules, policies, and procedures for your organization's business record e-mail, as well as Registered E-mail. Use your e-mail policy to spell out issues including usage (business and personal), content and netiquette, confidentiality rules, retention and deletion schedules, and litigationhold rules.

Develop your organization's strategic business record e-mail/Registered E-mail policies with regulatory compliance, litigation concerns, security challenges, privacy issues, and business needs clearly in mind. Assign a team of legal, compliance, IT, records management, and HR professionals to ensure that your company's e-mail/retention policies address all of the risks, rules, and regulations facing your business and industry.

Electronic communication policies should be clearly written and easy for employees to access, understand, and adhere to. Avoid vague language that may leave the organization's e-mail policy open to individual employee interpretation. Update written policies annually to ensure that your organization has rules, policies, and procedures in place to ensure compliance with any new regulations and the effective management of growing risks.

Distribute a hard copy of each written policy to all employees. Insist that every employee sign and date a copy of each policy, acknowledging that they have read the policy, understand it, and agree to comply with it or accept disciplinary action up to and including termination.

**2. Educate** employees. Support written rules and policies governing business record e-mail and Registered E-mail with companywide employee training. Make sure employees understand that e-mail and Registered E-mail policy compliance is mandatory, not optional. Thanks to policy training, employees are likely to be more compliant and the courts more accepting of the fact that your company has made a reasonable effort to manage Electronically Stored Information (ESI) effectively.

Based on the legal principle known as vicarious liability, an employer may be held responsible for the accidental or intentional misconduct of employees. That should be a wake-up call to the 48% of employers who do not educate employees about e-mail risks, rules and regulations, according to the American Management Association/ePolicy Institute research.

**Fully 43% of regulated employees don't adhere to record retention rules—or are unsure if they are in compliance. Another 34% of employees can't distinguish between business record e-mail that must be retained versus non-record messages that may be purged from the system.**

*Source: 2006 Workplace E-Mail, IM & Blog Survey, American Management Association/ePolicy Institute.*

Do not expect untrained employees to comply with policy that they may not understand—or may not even be aware of. Support electronic communication policies with employee education that addresses the following issues:

1. What is a business record? What is the organization's retention/deletion schedule? What is each employee's individual role in the retention/deletion process?
2. RPost Registered E-mail technology: How does it work? How does it differ from traditional e-mail? When and how should employees use it?
3. Review e-mail risks and liabilities facing the industry, organization, and individual users.
4. Spell out e-mail content, language, and netiquette rules.
5. Discuss e-mail ownership and privacy concerns: the organization's responsibilities and legal monitoring rights versus employees' privacy expectations.
6. Review industry and governmental regulations.
7. Explain e-mail's role as ESI—discoverable legal evidence.

8. Discuss confidentiality concerns. Stress the importance of protecting IP, trade secrets, company financials, proprietary information, confidential data, and internal documents.
9. Review monitoring laws, rules, and tools.
10. Discuss penalties—up to and including termination—awaiting those who violate record retention, e-mail acceptable usage, and RPost Registered E-mail usage policies.

**Enforce** your company's written electronic rules and policies with a combination of disciplinary action and technology tools including RPost Registered E-mail. Consistently apply discipline to show employees that management is serious about electronic communication policy compliance. Employers are getting tougher about policy compliance, with 26% of bosses reporting that they have dismissed employees for misusing the organization's e-mail system, according to 2006 American Management Association/ePolicy Institute research.

## Best Practices Review: Do's & Don'ts for Strategic E-Mail Management

### **DO:**

1. **Put E-Mail Policy In Writing.** Distribute a hard copy to all employees. Insist that every employee sign and date a copy, acknowledging that they have read the policy, understand it, and agree to comply with it or accept disciplinary action up to and including termination.
2. **Educate Employees About E-Mail Risks, Rules and Regulations.** Don't assume employees understand e-mail risks, rules and regulations. And don't expect them to comply with e-mail policy without training. Your company may need to demonstrate your commitment to employee education in court one day, so maintain a record of everyone who attends e-mail policy and compliance training.
3. **Incorporate E-Mail Retention Guidelines.** There is no one-size fits-all definition of a "business record." Create a definition of an e-mail business record for your organization, perhaps on a department by department basis. Establish e-mail business record retention rules, policies, and procedures for employees. Install software to automate retention/archiving, so your company can quickly and reliably locate and produce e-mail should a court or regulator subpoena it.

4. **Set Rules for Personal Use.** Spell out exactly how much personal e-mail use is allowed. Let employees know with whom they may communicate, under what circumstances, what topics they may and may not discuss, and when and for how long they may engage in personal e-mail. Use specific language that's not open to individual interpretation.
5. **Institute Clear Content Rules, Language Guidelines and Netiquette Policy.** Use e-mail policy to clearly define approved and banned language and content. Insist that employees behave professionally and adhere to content rules established by regulators and management. Establish netiquette guidelines to ensure that employees' e-mail communication adheres to the rules of civil business behavior.
6. **Minimize Privacy Violations by Educating Employees.** Depending upon your company's industry and regulatory requirements, be sure to educate employees about corporate, customer, patient and individual privacy/confidentiality risks, rules and regulations. Make sure employees know how to comply with the regulations, laws and policies governing protected health information, nonpublic personal information, copyright, intellectual property, etc.
7. **Address E-Mail Ownership, Monitoring and Employee Privacy Concerns.** The federal Electronic Communications Privacy Act (ECPA) gives U.S. employers the right to monitor employee e-mail. Use written policy to inform employees that they have no reasonable expectation of privacy when using the e-mail system. Inform employees that the company reserves the right to monitor, inspect, copy, review, and store at any time and without notice any and all e-mail. Also let employees know that management reserves the right to disclose e-mail text and images to regulators, the courts, law enforcement, and other third parties without the employee's consent.
8. **Be Sensitive to the Needs of Protecting Both Company and Employees when sending Important Business E-mail.** Simple e-mail messages are plain text format that can be altered and provide little evidentiary value with respect to proving delivery, content and time stamp. Use Registered E-mail in all instances where the loss of a legal/regulatory challenge stemming from an e-mail exchange could be costly to the company and/or deleterious to the employees' job status.

**DON'T:**

1. **Be Inconsistent.** Establish corporate rules, policies and procedures that apply to all employees, regardless of title or rank. Don't create separate

policies for executives. Don't allow individual offices to set their own e-mail policies. Be consistent when disciplining policy violators, too.

2. **Forget Your International Associates.** Some countries outlaw e-mail monitoring. If you have employees or offices operating abroad, be sure to have the legal team investigate the e-mail-related laws and regulations governing each country in which your organization has a presence. Then adapt international e-mail policies accordingly.
3. **Take Electronic Policy Enforcement Lightly.** Assign a team of legal, compliance, IT, HR, training and records management professionals the task of developing, implementing, and enforcing the organization's e-mail policy and procedures. Establish penalties for policy violations, and enforce those penalties consistently.
4. **Leave Compliance to Chance.** The most effective way to reduce e-mail risks is to combine written policy with ongoing employee education backed by content security software. Savvy employers apply this three-tiered approach to help prevent potentially costly and protracted disasters including regulatory investigations and workplace lawsuits.

## Sample E-Mail Policy

(Organization) is pleased to make e-mail access available to authorized employees. Created as a business tool to help (Organization) employees serve customers, communicate with suppliers, streamline internal communications, and reduce unnecessary paperwork, the e-mail system is intended primarily for business purposes. Personal use of (Organization's) e-mail system is restricted to the terms outlined below. The e-mail system is the property of (Organization). Employees accessing (Organization's) e-mail system are required to adhere to the following policy and procedures. Violation of (Organization's) e-mail policy may result in disciplinary action, up to and including termination.

1. All communications and information transmitted, received, or archived in (Organization's) computer system belong to the company. The federal Electronic Communications Privacy Act (ECPA) gives management the right to access and disclose all employee e-mail messages transmitted or received via the organization's computer system. (Organization) intends to exercise our legal right to monitor employees' e-mail activity. When it comes to e-mail, employees should have no expectation of privacy. Be aware that management may access and monitor e-mail at any time for any reason without notice.
2. The e-mail system is reserved primarily for business use. Only under the following circumstances may employees use (Organization's) e-mail system for personal reasons:
  - a) Communication with children, spouses, and immediate family is permitted but must be limited to no more than 15 minutes a day during business hours. Employees also are free to e-mail children, spouses, immediate family during the lunch hour and other authorized break times.
  - b) Personal e-mail communication that exceeds the time limits outlined in point 2a and/or which is conducted between the employee and an individual other than a child, spouse or immediate family member is prohibited unless authorized by (Organization's) human resources manager.
  - c) The use of (Organization's) e-mail system to solicit for any purpose, campaign for a political candidate, espouse political views, promote a religious cause, and or advertise the sale of merchandise is strictly prohibited without the prior approval of the Chief Information Officer.
3. If the e-mail commits the company to anything at all, send it as an RPost Registered E-mail message and retain the Registered Receipt e-mail as an evidentiary record of the correspondence.

4. E-mail passwords are the property of (Organization). Employees are required to provide the Chief Information Officer with current passwords. Only authorized personnel are permitted to use passwords to access another employee's e-mail without consent. Misuse of passwords, the sharing of passwords with non-employees, and/or the unauthorized use of another employee's password will result in disciplinary action, up to and including termination.
5. Privacy does not exist when using (Organization's) computer system including desktop computers, laptops, and handhelds. Confidential or personal information never should be sent via e-mail without the understanding that it can be intercepted. This includes the transmission of the organization's intellectual property, customer financial information, Social Security numbers, employee health records, proprietary data and trade secrets, and/or other confidential material. When sending confidential material (or any messages for that matter), employees should use extreme caution to ensure the intended recipient's e-mail address is correct.
6. Exercise sound judgment and common sense when distributing e-mail messages. 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. Exercise caution when sending blind carbon copies to ensure you don't violate addressees' privacy by inadvertently sending carbon copies.
7. E-mail usage must conform to (Organization's) harassment and discrimination policies. Messages containing defamatory, obscene, menacing, threatening, offensive, harassing, or otherwise objectionable and/or inappropriate statements--and/or messages that disclose personal information without authorization--are prohibited. If you receive this type of prohibited, unsolicited message, do not forward it. Notify your supervisor and/or the Chief Information Officer about the message. Delete the message as instructed by management.
8. E-mail messages should be treated as formal business documents, written in accordance with (Organization's) Electronic Writing Style and Netiquette Guidelines. Style, spelling, grammar, and punctuation should be appropriate and accurate, and the rules of netiquette must be adhered to.
9. Employees are prohibited from sending jokes via e-mail. Jokes, which often contain objectionable material, are easily misconstrued when communicated electronically.
10. Employees are prohibited from sending organization-wide e-mail messages to all employees without approval from the Chief Information Officer. In addition, employees are prohibited from requesting e-mail replies to organization-wide e-mail without the permission of the Chief Information Officer.
11. Employees may not waste (Organization's) computer resources or colleagues' time. Send e-mail messages and copies only to those with a legitimate need to

read your message. Chain messages and executable graphics should be deleted, not forwarded, as they can overload the system.

12. Only the Chief Information Officer and/or Systems Administrator may generate public e-mail distribution lists.
13. Employees are responsible for knowing and adhering to (Organization's) e-mail retention and deletion policies.
14. Misuse and/or abuse of (Organization's) electronic assets (wasting productive time online, copying or downloading copyrighted materials, visiting inappropriate sites, sending inappropriate/abusive e-mail messages, etc.) will result in disciplinary action, up to and including termination.

*Employee Acknowledgment*

Note: If you have questions or concerns about (Organization's) E-Mail Policy, contact the Chief Information Officer and/or Human Resources Director before signing this agreement.

I have read (Organization's) E-Mail 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

Source: ©2007, The ePolicy Institute (www.epolicyinstitute.com or 614-451-3200), Executive Director Nancy Flynn. For informational purposes only. Individual policies should be developed with assistance from competent legal counsel.

## The ePolicy Institute

The ePolicy Institute is dedicated to helping employers limit electronic risks, including litigation, through the development and implementation of Electronic Communication Policies and employee training programs.

The ePolicy Institute is often asked to recommend technology solutions that present simple to implement, effective solutions to electronic risks. In this guide, the ePolicy Institute has recommended use of RPost® ([www.rpost.com](http://www.rpost.com)) Registered E-mail® services. RPost's patented services provide the sender with legally valid evidence of precisely what e-mail content and attachments were sent and received, by whom and when. RPost services include an integrated set of eContracting, e-signature, security and privacy/encryption tools. Available in six languages, RPost Registered E-mail® services are also used daily by the United States Government and have been endorsed and marketed by many of the influential bar associations in the United States.

An international speaker and trainer, ePolicy Institute Executive Director Nancy Flynn is the author of 8 books published in 5 languages. As a recognized authority on workplace e-mail/IM/blog/Internet usage, Nancy Flynn is a popular media source who has been interviewed by *Fortune*, *Time*, *Financial Times*, *NewsWeek*, *The Wall Street Journal*, *US News & World Report*, *Business Week*, *USA Today*, *New York Times*, National Public Radio, CNBC, CNN, CBS, ABC, NBC, and Fox News among others. **Top Tips for E-Mail Management** is based on material excerpted from author Nancy Flynn's books *E-Mail Rules*, *Instant Messaging Rules*, *Blog Rules*, *The ePolicy Handbook*, *Writing Effective E-Mail*, and *E-Mail Management*. Contact Nancy Flynn about ePolicy Institute training, products & services (614-451-3200) or [nancy@epolicyinstitute.com](mailto:nancy@epolicyinstitute.com).

[www.epolicyinstitute.com](http://www.epolicyinstitute.com)

"REGISTERED E-MAIL" is a trademark owed by RPost