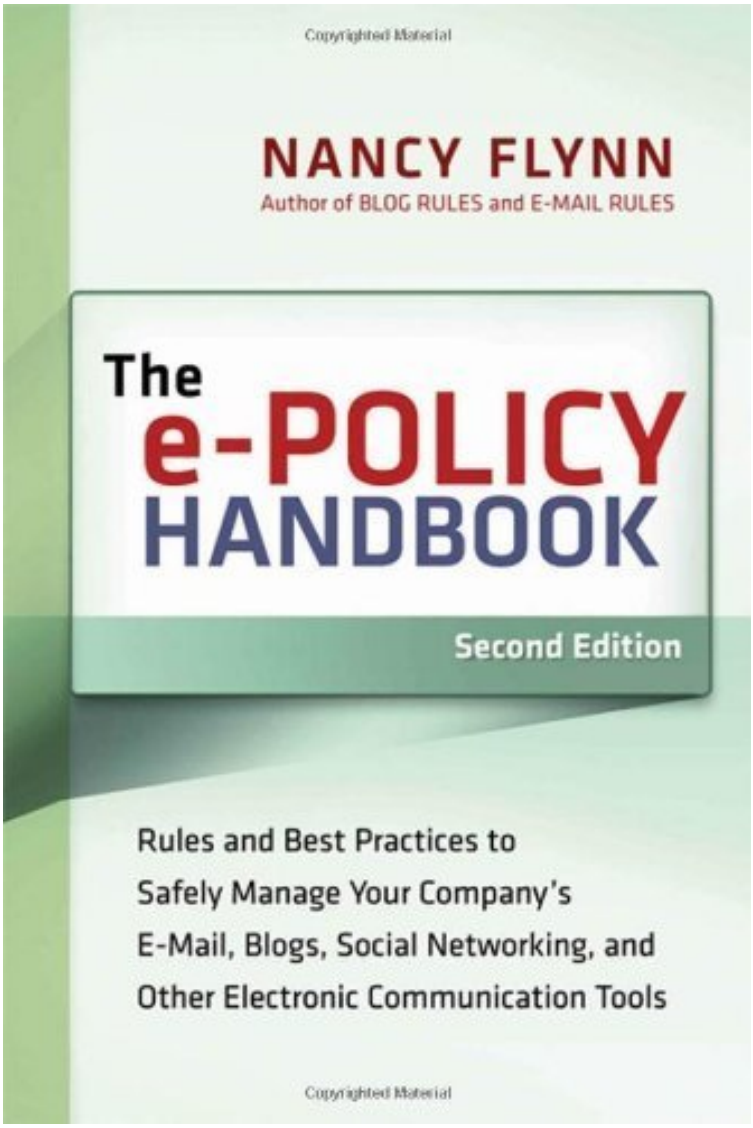
The e-Policy Handbook: Rules and Best Practices to Safely Manage Your Company's E-Mail, Blogs, Social Networking, and Other Electronic Communication Tools

Nancy Flynn



#1753478 in eBooks 2009-01-07 2009-01-07File Name: B002GEDUQO | File size: 73.Mb

Nancy Flynn : The e-Policy Handbook: Rules and Best Practices to Safely Manage Your Company's E-Mail, Blogs, Social Networking, and Other Electronic Communication Tools before purchasing it in order to gage whether or not it would be worth my time, and all praised The e-Policy Handbook: Rules and Best Practices to Safely Manage Your Company's E-Mail, Blogs, Social Networking, and Other Electronic Communication Tools:

1 of 1 people found the following review helpful. A must have for an office manager.By CustomerFun, concrete, easy to read. I'm writing my office email policy based im this book.0 of 0 people found the following review helpful. Step-by-step training and sample policies along with real-world case histories makes for a fine surveyBy Midwest Book ReviewDigital abuse can tear companies apart - such abuse includes software pirating, inappropriate e-mails, and more. Businesses seeking protection from liability need the latest updated edition of The e-Policy Handbook: it has been newly updated to reflect the latest electronic developments and offers strategies for identifying and preventing data theft, customer information, and more. Step-by-step training and sample policies along with real-world case histories makes for a fine survey.0 of 4 people found the following review helpful. FUDBy JAYNESS the GreatFear, uncertainty, and doubt. That's what the author is selling. According to her, anything that can go wrong is certain to happen and anything that can't go wrong, might happen. If you enforced her recommendations at a company, everyone would quit and you would be fired. Run away from this book as hard and as fast as you can.

" Trillions of e-mails travel each year through corporate networksmdash;and they're not all work-related. But for organizations wishing to protect themselves from liability, e-mail is no longer the only dangermdash;they now have to contend with blogs, social networking sites, and other new technologies. Packed with electronic rules, step-by-step guidelines, sample policies, and e-disaster stories, this revised edition of The e-Policy Handbook helps readers:implement strategic electronic rules bull; prevent security breaches and data theft bull; safeguard confidential company and customer information bull; manage new and emerging technologies bull; write and implement effective policies bull; train employeesUpdated to cover new technologies, including instant messaging, social networking, text messaging, video sites, and more, this is a comprehensive resource for developing clear, complete e-policies. "

From the Back Cover With trillions of e-mails traveling each year through your corporate networkmdash;and not all of them work-relatedmdash;your company can be left wide open to liability risks, security breaches, and productivity nosedives. And now, with the advent of blogs, social networking sites, and other new technologies, e-mail is no longer the only danger! Newly updated to cover the latest threats to your organizationrsquo;s security, including instant messaging, text messaging, video sites, and more, The e-Policy Handbook gives you everyshy;thing you need to develop clear, complete e-policies. Packed with electronic rules, step-by-step guidelines, sample policies, and e-disaster stories, this new edition shows how to: mdash;nbsp;nbsp;nbsp; implement strategic electronic rules mdash;nbsp;nbsp;nbsp; understand ldquo;cyber-lawsrdquo; mdash;nbsp;nbsp;nbsp; prevent security breachshy;es and data theft mdash;nbsp;nbsp;nbsp; safeguard confidential company and customer inforshy;mation mdash;nbsp;nbsp;nbsp; manage new and emerging technologies mdash;nbsp;nbsp;nbsp; write and implement effective policies mdash;nbsp;nbsp;nbsp; train employshy;ees about your companyrsquo;s online rules nbsp; From off-color jokes to pornographic images, from software pirates to eBay addicts, digital abuse can tear any company apart. This thorough, up-to-date survival kit shows you how to protect your organization. nbsp; Praise for the First Edition of The e-Policy Handbook: nbsp; ldquo;What every business book should be: easy to understand, full of practical tips, and provocashy;tivehellip;.You might not find a more useful business book this year, or next, than this one.rdquo; mdash; Training nbsp; ldquo;If your company has an online presencemdash;even one employee onlinemdash;then buy this book.rdquo; mdash;nbsp;nbsp;nbsp; The Toronto Star nbsp; ldquo;The book is a timely and comprehensive survival kit showing how to adopt and monitor effective e-policies without alienating a workforce that grew up in the computer age.rdquo;nbsp;nbsp;nbsp; mdash;nbsp;nbsp;nbsp; Office Solutions ldquo;The e-Policy Handbook is the perfect companion to have at your side when drawing up your policies.rdquo;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp; mdash; Legal Management nbsp; ldquo;An eye-opening book.rdquo; nbsp;nbsp;nbsp;nbsp;nbsp;nbsp;nbsp; mdash; BookPage nbsp; Nancy Flynn is founder and executive director of the ePolicy Institutetrade;, www.epolicyinstitute.com, a leading source of e-mail- and Internet-related speaking, training, and consulting services. She is regularly quoted in major media, including Fortune, Time, The New York Times, The Wall Street Journal, USA Today, NPR, and CNN. Her books include Blog Rules and E-Mail Rules. She lives in Columbus, Ohio. About the Author Nancy Flynn (Columbus, OH) is founder and executive director of The ePolicy Institutetrade;, a leading source of e-mail- and Internet-related products and services. She is regularly quoted in major media including The Chicago Tribune, The New York Times, The Los Angeles Times , USA Today, NPR, and CNN. Her books include Blog Rules (978-0-8144-7355-9), and E-Mail Rules (978-0-8144-7188-3). Excerpt. copy; Reprinted by permission. All rights reserved. C H A P T E R 1 Why Every Organization Needs Electronic Rules and Policies Based on Best Practices Since the initial publication of The e-Policy Handbook in 2001, electronic business communication tools and technologies have taken the workplace by storm. Consequently, many employers find themselves drowning in risk as they struggle to manage the usemdash;and curtail the abuse mdash;of what were originally conceived as time-saving, productivity-enhancing technology tools. Without question, e-mail has become the business worldrsquo;s communication tool of choice, forever altering the ways in which we exchange information and conduct professional and personal relationships. Meanwhile, new tools and technologiesmdash;instant messenger (IM), blogs, social networking and video sites, cell phones and camera phones,

text messaging, lsquo;lsquo;confidentialrsquo;rsquo; electronic messaging, and the BlackBerry Smartphone, to name a fewmdash;have joined the electronic business communication mix at a breakneck pace. The good news: The ever-expanding universe of high-tech tools facilitates usersrsquo; ability to quickly and conveniently transmit business-critical data and stay connected with colleagues and customers around the globe. The bad news: Emerging technologies dramatically increase employersrsquo; exposure to potentially costly and protracted risks including workplace lawsuits, regulatory fines, security breaches, and productivity drains, among others. Fortunately, for savvy employers determined to manage technology use and minimize risks, there is a solution. Through the strategic implementation of a comprehensive e-policy program that combines written electronic rules with formal employee training supported by policy- based monitoring, management, and archiving tools, organizations can effectively minimize (and in some cases prevent) electronic risks while maximizing compliance with legal, regulatory, and organizational guidelines. e-Policy Rule 1: Through the implementation of a comprehensive e-policy program that combines written rules with employee education supported by discipline and technology tools, organizations can effectively minimize electronic risks and maximize compliance. In the Electronic Office, Risks Abound Even if your organization does not currently use IM, operate a business blog, or provide executives with BlackBerry Smartphones, you cannot afford to ignore new and emerging technology. If you fail to provide the hot, must-have technologies of the day, chances are your tech-savvy employees (particularly younger employees whose social lives revolve around IMing, texting, and social networking) will bring them in through the back door and load them onto your system without management approval or IT oversight. Left undetected and unmanaged, thatrsquo;s a recipe for disaster! Manage Powerful, Popular Electronic Business Communication Tools Proactively Considering that the average personal computer can hold 1 million pages of information, itrsquo;s no surprise that 90 percent of the business documents we create and acquire are electronic, according to the Association of Records Managers and Administrators (ARMA) as reported by Baseline Magazine.1 Employers who are concerned about managing all that electronic informationmdash;and related risksmdash;should act now to put written policies in place governing the use of established tools and new technologies at work during business hours and at home on employeesrsquo; own time. Old and new alike, all electronic business communication tools must be addressed by comprehensive, best-practices-based rules and policies as detailed in this book. Failure to establish and enforce written rules and e-policies puts the organization at risk of electronic disasters including, but not limited to: regulatory audits, security breaches, lost productivity, shattered stock valuation, negative publicity, lost credibility, and workplace lawsuits, which employers and legal professionals alike consistently identify as their number-one e-mail and Internet-related concern. 2 e-Policy Rule 2: You cannot afford to ignore new and emerging technology. If you fail to provide the hot, must-have technologies of the day, chances are your tech-savvy employees will bring them in through the back door. Left undetected and unmanaged, thatrsquo;s a recipe for disaster! Employers Face Ever-Increasing Legal Liability As early as 2001, when the first edition of The e-Policy Handbook was published, employers cited legal liability as their primary reason for monitoring employee e-mail and Internet use.3 Since then, we have witnessed the expanding role of e-mail and other forms of electronically stored information (ESI) as evidence in civil lawsuits and criminal trials. In 2006, 24 percent of organizations had employee e-mail subpoenaed, compared to just 9 percent in 2001. Another 15 percent of companies went to court to battle lawsuits specifically triggered by employee e-mail in 2006, according to the Workplace E-Mail, Instant Messaging, and Blog Survey from American Management Association and ePolicy Institute.4 Electronically Stored Information Plays an Ever-Expanding Evidentiary Role There is no doubt that the evidentiary role of workplace e-mail and other electronically stored information will continue to expand. The United States Federal Court made clear this fact in December 2006, when the much-anticipated amendments to the Federal Rules of Civil Procedure (FRCP) were announced, affirming the fact that all electronically stored information is subject to discovery (which means it may be subpoenaed and used as evidence) in federal litigation. When it comes to electronic evidence, it is the content that counts, not the tool or technology used. Whether created, transmitted, acquired, posted, downloaded, or uploaded via e-mail, IM, the Internet, a cell phone, or any other tool, ESI creates the electronic equivalent of DNA evidence. ESI canmdash;and willmdash;be subpoenaed and used as evidence for or against your company should it one day become embroiled in a workplace lawsuit. Will you be prepared? e-Policy Rule 3: Electronically stored information (ESI) creates the electronic equivalent of DNA evidence. ESI canmdash;and willmdash;be