



The
BUSINESS RECORDS MANAGEMENT
BULLETIN



A Service of **BUSINESS RECORDS MANAGEMENT LLC**

2nd Quarter 2009

COMMUNICATING E-MAIL MANAGEMENT

Like a horror-movie creature from the grave that can't be killed, e-mail is the wraith that persists beyond the boundaries of your organization in someone's "in" box even though you've managed to delete it inside your corporate structure. The ghost of e-mail can disappear into the ethernet, beyond grasp when it is needed as evidence in a court case. In recent years huge corporations have been fined millions of dollars because they were unable to produce e-mail files in high profile cases, or because they deleted e-mail that was designated as discovery (spoliation).

Managing e-mail has become a major concern for most organizations. There are thousands of technological methods that can be applied. But it takes the right kind of employee mindset to make these methods work. This is where communicating the management policy enters in.

Nancy Flynn is executive director of The ePolicy Institute which studies workplace policies for e-mail and web usage and produces business guides on these topics, with the support of MessageLabs. Her downloadable white paper titled "Not Just Words: Enforce Your Email and Web Acceptable Usage Policies" sets forth the reasons for having such policies, and enforcing them, to reduce business and security risks. These rules are enhanced by statistics taken from a 2007 survey on electronic monitoring and surveillance conducted by the American Management Association and The ePolicy Institute.

An Acceptable Usage Policy, AUP, should be written clearly and specifically so that there will be no gray areas that can be open to interpretation in the mind of an employee at the time of an action that may bring harm to the organization. Control of written content in e-mail is necessary and must be backed up by 100 percent compliance. Of the surveyed managers who had fired staff for violating e-mail rules, 62 percent cited off-color language or content as the reason.



Such incidents are embarrassing. But a greater danger awaits regulated industries or publicly held companies if confidential information is leaked in violation of securities laws. Or if proprietary information is given to outsiders.

Flynn states that personal use of e-mail and the web increases risk for the organization. Excessive time spent on e-mail or the web is unproductive, takes up space on the system, and may produce legal evidence if personal e-mails are archived with business e-mails that could be open to discovery.

Employees Cannot Expect Privacy

In the United States, employers have a right to monitor all the activities that an employee may perform on a company owned computer system. Some employers use technology to monitor external e-mail, but many do not monitor internal e-mail. Of the surveyed employers who monitored incoming and outgoing messages, only 50 percent monitored e-mail among employees. To control content, MessageLabs offers services such as search tools that will look for predetermined words or phrases, or which will spot unusually large attachments.

It comes as a shock to many employees to learn that

they have no grounds for privacy when they are using a company's computer system to do any kind of electronic communication, for business or for personal reasons. Of the employers surveyed, 24 percent had faced subpoenas for an employee's e-mail, and 15 percent had been forced into court over employee e-mail.

For those employees who work for governments at any level, e-mail privacy does not exist because their emails are open records and can be accessed by taxpayers and the media, thanks to state and federal Freedom of Information statutes. For this reason records managers for state governments have developed e-mail policies to fit the open access legal frameworks of their states. In South Carolina, the Department of Archives and History says that an email retention policy must include information on access because government e-mail can be defined as a public record subject to the Freedom of Information Act and Public Records Act. However, some information is considered personal or private, and thus could be exempt from disclosure as set forth by FOIA and HIPAA. E-mails may be subject to legal discovery, and those stored at multiple locations, even though deleted by their originator, may be recoverable for court. (www.state.sc.us/scdah.)

In Minnesota, a legal framework for e-mail management will be drawn not only from the Official Records Act and the Records Management Act but also the Minnesota Government Data Practices Act stating that government records must be accessible to the public unless categorized as not-public by the state legislature, with caveats because e-mail is so easily forwarded, misdirected and sent to groups of people.

The policy further stresses security for e-mail records with controlled access, storage, retrieval, alteration, and deletion—again particularly as it relates to notpublic e-mails. (www.mnhs.org.)

What can an e-mail archiving system do for you?

It is a necessity for meeting compliance requirements, in the view of Quest Software, not only because it captures and locates information but because it also centralizes control of the e-mail system and thus undergirds the Acceptable Usage Policy. It lessens the chance that an e-mail will be kept in offline or personal stores outside your corporate boundaries, where it will still exist although it has been deleted within your organization's system. If you don't know where it is, it could be subject to discovery and become an unpleasant surprise. (www.quest.com)

But...is e-mail the right way to send your message?

An interesting and thoughtful article presented by ITtoolkit.com asks questions about e-mail etiquette. Yes, e-mail is fast and easy, but is it the correct way to send the message you want to impart? Could it be viewed as slapdash and inappropriate? Here are some things to consider.

- E-mail may seem too casual for certain types of information, and that could lessen the perceived value of your message.
- Your message as an e-mail may get lost in an overcrowded mailbox.
- If your message contains confidential or personally sensitive information, to preserve privacy you should not use e-mail. Your company may have internal policies for how such information should be handled.
- How is e-mail viewed within the corporate culture of your organization? What is the company attitude about e-mail? Are there some who do not use it?
- To do justice to the message you want to send, consider this checklist that asks questions as to: audience, purpose, topic and timing, content and format.
- What is your relationship with the person you are sending this to, or the group of persons. Do you know how he, she or they would react to getting this information by e-mail? If there are primary recipients plus those who are cc'd, and those who are bc'd, could this possibly be forwarded to others that you do not know?
- What is the purpose of this message—to give information, request something, say thank you, or is there another reason?
- Is this message urgent and are you asking for a response by a certain time?
- How can this message be written so its intention is clear to all and will not be misunderstood? This may take some writing and rewriting on your part.

If you choose e-mail, be sure it is grammatically correct and spell-checked. If you "dress for the job you want, not the job you have," then use your e-mails to strive for the job and influence you want, not the one you have. (www.ittoolkit.com)

Ask for help with your e-mail management needs.

Your storage contractor can offer tips on developing a policy for e-mail management or strengthening the policy you have. E-mail management is a necessary part of risk management. Organizations Need to Reduce Cost and Risk

Organizations Need to Reduce Cost and Risk of Managing Electronic Information

The non-profit industry association AIIM introduces new and improved Electronic Records Management training course.

Share! Print

“Organizations are drowning in electronic information such as emails, office documents, instant messaging, images and blogs, and mismanagement of business information can seriously damage organizations but also careers,” states John Mancini, President of AIIM, a nonprofit association for information management. “Most business records are now born digital and the exponentially increasing volume and types place a huge challenge for organizations.”

Mancini recommends executives to ask the following 3 questions to identify their confidence in electronic records:

- Has your ability to document what your organization did, why you did it, who did it, and when they did it gotten better or worse in the past 5 years?
- Is your organization able to handle the explosion of digital information and records, or does the continuing influx of information make your organization less and less effective?
- Can your executives, staff, and legal counsel find electronic records when they need it? In the daily course of business, as well as when an emergency or more urgent event occurs?

“Increasing awareness is one key reason why AIIM has introduced online and classroom training programs covering how to identify and manage electronic records,” states Bob Larrivee, Director, of AIIM. “Close to 10,000 IT, business and information managers have attended the AIIM Certificate Programs over the last 3 years, and AIIM’s introduction of a new and improved AIIM Electronic Records Management (ERM) Certificate Program incorporates timely and emerging best practices and technologies for managing electronic records. More than 50% of the program content has been changed or

improved based on feedback from AIIM’s Education Advisory Groups.”

According to Larrivee, “Students, who have completed the ERM program prior to now, should consider taking this updated version to enhance their skills and strengthen what they learned in the prior course.”

The new and improved ERM Certificate Program covers:

- SharePoint, ECM, and ERM solutions for managing electronic records
- Retention schedule and disposition
- Metadata model, classification scheme and access control
- Digital preservation techniques
- Global best practices for implementation ERM
- Email capture and retention
- Impact of new content types such as wikis and blogs

The newly revised ERM Certificate Program is available at the Practitioner and Specialist levels to students through instructor led classroom sessions and on-line at www.aiim.org/training. The Masters program is available through instructor led classroom sessions only. Those wishing to inquire about private classes can contact AIIM directly.

About AIIM

AIIM (www.aiim.org) is the community that provides education, research, and best practices to help organizations find, control, and optimize their information.

The AIIM community has grown to over 65,000 professionals from all industries and government, in over 150 unique countries, and within all levels of management including senior executives, line-of-business, and IT.

For over 60 years, AIIM has been the leading non-profit organization focused on helping users to understand the challenges associated with managing documents, content, records, and business processes. Today, AIIM is international in scope, independent, implementation-focused, and, as the representative of the entire enterprise content management (ECM) industry - including users, suppliers, and the channel - acts as the industry’s intermediary.

BRM partners with NAPO (National Association of Professional Organizers) for Shred Day Event



On Saturday April 18th, BRM held a shred day in conjunction with the National Association of Professional Organizers (NAPO) at the Staples on Banksville Road in the South Hills and the Staples at the Waterworks Mall. From 10am-2pm, BRM and NAPO collected paper items from the public to be shredded. The event was very successful, collecting approximately 12,000lbs of paper from both locations combined. BRM hopes to partner with NAPO in the future for another shred event.



BUSINESS RECORDS MANAGEMENT
BRM Disaster Recovery Services

1018 Western Avenue
Pittsburgh, PA 15233
Ph: 412-321-0600
Fax: 412-321-5152
www.businessrecords.com