www.notationsonnonprofits.com

"I'm Supposed To Keep Those Emails?" The Need For An Electronic Document Policy

What is That Exactly?

What constitutes as an electronic document or record is massive.

There's the stuff we tend to think of like emails, databases, word processing documents and spreadsheets. But what many don't think about are the blogs, chat room transcripts, instant messaging transcripts, voice-mails, text-messages and even deleted documents. All this has to be kept somewhere, ready to accessed and destroyed when appropriate.

Even more of a mind boggle is grasping how electronic documents and records are created and where they are stored; desktops (both at home and work), laptops (both at home and work), servers, iPods, touches, cell phones, tablets, USB's, hard-drives, CD's, clouds (online and servers), fax machines and copiers, IM and Chat applications, Internet Browsers, websites.....whew.

So What?

For organizations the question becomes: do you know where these documents are being generated and who has access to them?

Increasingly organizations are opting to go paperless, and now, more than ever, documents are likely to be generated and kept in electronic format. And less than 30% of them are ever printed out.

There are dozens of reasons why knowing how your electronic documents are generated, stored and destroyed is important. A few being:

- If the organization is subpoenaed for information. Even if you're not getting sued, there are instances where the court may subpoena you for information that needs to be at the ready.
- If a government agency or grant organization wants to conduct an audit be it financials, compliance or both. You'll want to be able to quickly pull the information they need.

- In case the organization is sued and has to produce documents. Oftentimes, if a document is needed for litigation (for example a personnel record for a wrongful termination suit) and you've unreasonably destroyed it a court can give the jury instructions to essentially presume the document was incriminating. I wrote on a specific case where that happened here.
- Such knowledge may be mandated by state and/or federal law. Statutes like OSHA, Sarbanes-Oxley, Gramm-Leach and HIPAA, or agencies like the IRS and State Attorney General's Office each, in their own way and to their own degree, address how organizations must maintain and destroy certain information.
- Lastly, and closer to home, imagine how catastrophic it would be if the intern that just left had the only copy of last year's gala attendees? Or worse, people who gave to the organization? How much would you love to be able to pull up whatever you wanted in just a few clicks?

What You Can Do?

You'll want to consider implementing a document or records management policy. If you already have one in place then you'll want to ensure certain portions are tailored specifically for electronic documents and records. Organizations often think about systems for paper documents, but fail to think about all the electronic documents and records they're generating that need to be accounted for.

I know, I know. How exactly are you supposed to do that when your staff is comprised of you, an intern and your spouse part-time?

Despite what you might have read thus far, this doesn't have to be an enterprise effort and can sound much bigger than it has to be. These type of processes work best when carefully tailored. So if you don't generate as much as Susan G. Komen, there's no need to implement a process on that scale.

You'll want to identify where the records are being generated, then how they're being filed, where they're being kept and ultimately how destruction takes place.

But the intangible nature of these documents and records will make how they're handled one of the most important stages to understand. Once you've gotten a grip on that, being pre-emptive and instructive will be key in getting and maintaining control.

In this regard, employees, volunteers, contractors and board members will be a huge factor. Is anyone issued an organization laptop? Is software installed that captures what is being generated? Are documents being backed up to a central server or cloud for access? Are people being allowed to download one of the several gazillion IM or chat apps? Essentially, are you giving someone the ability to put the organization at risk? Whether that risk be legal, regulatory or succession oriented?

One form of protection would be placing restrictions on the use of computers. This is where a policy will help. Stipulate that the employee has no right to expect any privacy. Address what type of documents can be generated using the organization's equipment (not just on the organization's premises) and for what purposes

the equipment may be used. You'll also want to create a protocol as to how documents must be generated, stored on the computer and perhaps you could even create a standard naming system.

Another trick would be utilizing the technology computers are coming with. Many of the newer computers are starting to come with really snazzy features that allow you, as an admin, to control what other users may and may not download.

A Few Parting Things You'll Want to Keep In Mind...

...when developing a plan.

- Be weary of generic retention plans. This is something that takes some thought. Particularly since so much of what you do will depend how and where you operate. There will be statutes of limitations specific to the city and state you're in. And if you're collecting sensitive information such as that dealing with health or one's finances then there will be federal regulations you have to consider.
- Deleted records will be the trickiest. If you've been paying attention to the whole "meta-data" topic, it's tremendously hard to actually "delete" a document off a hard-drive. In fact, in recent experiments conducted on disposed hard-drives, astonishing numbers of them usually still have data on them. This article Designing a Computer Electronic Record provides fantastic and economical solutions for this.
- Realize destruction of electronic information or records is not a menial task to be left to the intern. As the author notes in the article above, there is definitely an economic incentive for someone to take information being disposed of and use it. Best that it's handled by someone high up in the organization.
- A retention program for your electronic records and information will be, and should be, different than that for paper.
- Bear in mind, timely destruction of documents is just as important as maintenance.
- Understand, a document retention program is not "oh this looks bad let me throw it away". It must be reasonable and there must be a standard process that is adhered to.
- Lastly, conduct periodic audits to ensure that what you've put in place actually works for you. If something isn't being kept long enough (for example you find that for operational needs donor or or grant-maker lists need to be kept longer) than do so.

Sources: Computer Technology Review, March, 2003, by Sharon Isaacson, Criminal Investigation, October ,2003, Laura French

Other Posts You Might Like

Have You: Drafted a Records Management Policy?

Privacy Policies For Non-Profits: Sample & Resources

Hours, Sch-mours. Why You Really Should Be Keeping Track

Have You: Developed Good Intern Policies?