https://www.americanexpress.com/us/small-business/openforum/articles/handling-company-vs-private-email/

What to Consider When Handling Company Vs. Private Email

Julie Bawden Davis
Writer/Author/Publisher/Speaker, Garden Guides Press

Do you know your responsibilities as a business owner when it comes to private and company emails? Here are elements to consider when it comes to establishing and communicating your policy.
March 13, 2015

As recent headlines show, public officials can catch heat regarding using private rather than government email addresses to conduct business. What about small-business owners and their employees? Just what are the rules and regulations when it comes to your company email?

The Federal Records Act requires that emails of federal officials be public so that anyone who wishes to—including other government officials, news media and historians—can access them. Small-business owners may not have to worry about constituents, but they do have partners, employees, investors and possibly board members to answer to. And most small businesses have classified, sensitive and proprietary materials that shouldn't get into the wrong hands.

Here are some tips to help you stay out of hot water when it comes to your and your employees' email accounts.

Draw a Definite Line Between Private and Company Email

No good can come out of mixing private and company emails. As a business owner, it's best to delineate between the two, according to Eldonna Lewis-Fernandez, a veteran negotiation and contracts expert and author of *Think Like a Negotiator*.

"As a corporate employee who was building a business while working a corporate job, I had to toggle between two worlds," Lewis-Fernandez says. "I could not use my corporate email for personal use and could not use my personal email for corporate use.

"The biggest concern when using your personal email for official business is the inability to track it and the possibility of information getting hacked and sensitive information getting in the wrong hands," she adds. "This is why safeguarding of information is so critical, and keeping your official business official is paramount to protecting not only your company or organization but also yourself."

Know Employee Email Rights

As an employer, you have the legal right to monitor employee emails on your company's email system. Doing so can ensure that company proprietary information remains safe, and monitoring may enable you to head off trouble that might be brewing. At the same time, it's also important to note employee email rights.

For example, according to a ruling in January 2015 by the National Labor Relations Board (NLRB), your employees have the right to email amongst themselves regarding organizing a union and other similar activities that are protected under the National Labor Relations Act.

Provide Employees With Email Guidelines

"Email remains the go-to form of online communication and often involves the transfer of sensitive and proprietary business information in both text and file format," says Robert Rasmussen, COO of Balboa Capital. "Because of this, it is imperative that businesses have an iron-clad policy regarding the use of company and personal email. The email policy should be approved by company executives and a legal counsel, and be included in their employee handbooks."

You should provide employees with clear guidelines regarding company email use in your employee handbook. This can help ensure that employees abide by email protocol that's best for the company and can protect your business if a legal issue arises regarding email.

In the employee email guidelines, spell out rules regarding company email use. Note when they should use company email and when it's best to use private email. Also cover when it's acceptable to forward company emails and to whom. In addition, make it clear to employees that their company email is being monitored.

Protect Company Information

The misuse of email can present companies with a number of security and legal risks, Rasmussen suggests. "If an employee sends an email containing confidential information over an untrusted network that does not have the necessary security protocols, it can be read or copied during transmission," he says.

Rasmussen advises that small businesses have their IT departments use best practices when it comes to securing and monitoring email communication.

"Network infrastructures should be equipped with firewalls, routers and anti-virus software," he says. "For an added layer of protection, the mail server application and mail client application can be secured and email encryption technology can be deployed."

No Virtual Communication Is Truly Private

The bottom line is that any correspondence put into cyberspace—be it in a company or “private” email—is not private, advises leadership expert Roxi Bahar Hewertson, author of *Lead Like It Matters...Because It Does*.

“Anything we write or say electronically is recorded somewhere, like it or not," she says. "If you don't want it to show up on the front page of *The New York Times*, then don't write it or say it in an email or text.”

Read more articles on cyber security.

Photo: iStockphoto