BusinessManagement DAILY

APRIL 8, 2020

New rules of email: Managing email risks during the coronavirus crisis

With so many employees working from home during the coronavirus crisis, the time is right for an email refresher. Your organization's employees must maintain professional email communications with coworkers and clients, whether working from cubicles or couches. Here are four rules to help ensure employees create businesslike, compliant email—even when working at their kitchen tables.

1. **Enforce email policy.** Whether at headquarters or home, employees must adhere to the organization's email policy. Make sure remote workers understand that policy compliance is mandatory, whether using the company's email systems, accounts, and devices or their own personal tools and technologies. Conduct online training to remind remote employees of the many federal/state laws and industry/government regulations governing email content, use, and records. You don't want to lose otherwise-valuable staff over at-home email policy violations.

2. **Explain how business record email differs from non-record messaging**. Do your employees know that email creates business records, which the organization is required to protect and preserve for legal and regulatory reasons? Mismanaged, misplaced, or missing email records are more than a nuisance. They are a liability. Failure to manage email records compliantly could result in costly court sanctions, regulatory fines, and lost revenues. Protect your organization's business records by requiring at-home workers to attend online record retention training. Emphasize the fact that email users must comply with the organization's record retention policy, both at the office and at home. Make sure everyone knows their individual record retention/deletion roles and responsibilities. Record management is a must for business—even in the face of a pandemic.

3. **Impose security rules on home tools.** Email users working from home are responsible for protecting the organization's business records, as well as the privacy of customers, consumers, and coworkers. Safeguard the integrity of business information by imposing security rules on remote workers. Do not allow employees' families, roommates, or friends to use any personal mobile devices that are intended for business. Require shelter-at-home staff to password-protect home computers and personally owned mobile devices that are used for business. Have your IT department equip remote workers' home computers and personal mobile devices with software designed to block viruses, malware, spyware, malicious intruders, and other threats. Conduct online training on the organization's computer security policy, confidential and sensitive information policy, password procedures, and other guidelines designed to protect business records and individual information.

4. **Insist on effective error-free email.** In the battle for the reader's time and attention, polished writing counts. Unprofessional email communications can drive away customers, confuse colleagues, and derail careers. Email writing projects an image (positive or negative) of the individual and the organization. Effectively written email that is free from grammar goofs, spelling slip-ups, and punctuation problems is sure to command reader respect. Take advantage of stay-at-home orders and conduct web-based writing effective email training to help keep employees' email error-free, polished, and professional. For a free

copy of the tip sheet, *Great Grammar in Seven Steps*, email Nancy Flynn at Nancy@ePolicyInstitute.com.