Effective Email Policy Guidelines

for your business

FocusDataSolutions

The internet and electronic communication have revolutionized the way we conduct business, and it is important to have company policies that help employees understand how they should use (and not use) these powerful tools. At their best, these tools make us efficient, productive and better informed. Misuse, however, can create problems that distract from and undermine a company's mission.

An effective email policy

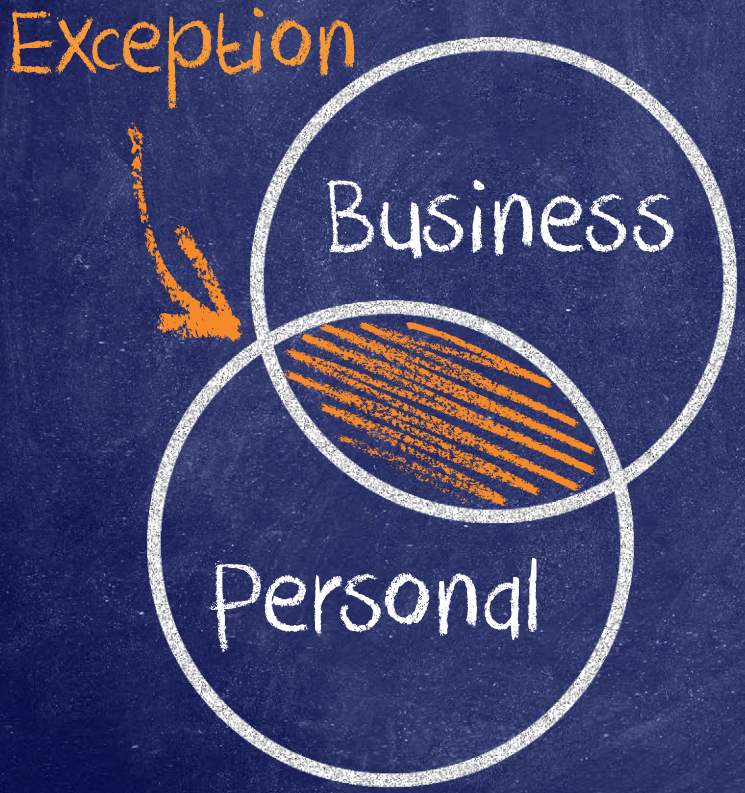
will encourage positive, productive communications while protecting a company from legal liability, reputational damage and security breaches. Like most company policies, rules and expectations should be tailored to fit the needs of the business and industry in which it operates. Below, we discuss the potential components of a company email policy recognizing that each business will have to determine what is most important and relevant to their organization.

Where to begin?

To determine the answer to the question above -- what are the most relevant and important components to include in your company's email policy? -- gathering the input of various stakeholders in the company may help. The HR department, IT department, management, PR experts, legal counsel and others may have important contributions.

The email policy should be compatible with other office policies, such as rules related to harassment, company communications and document retention. Making the policy succinct and easy to understand (and therefore easy to follow) is an important consideration, as well as the effect it will likely have on employee morale. Since technology changes rapidly, email policies should be regularly reviewed and updated. As with any policies an employer imposes on its employees, legal counsel is essential.

1 Business Use and Personal Exceptions



First and foremost, it should be clear, though it may seem obvious, that the use of a business email address is for business purposes – that is, to conduct business on behalf of the employer in line with the employee's responsibilities.

A business may want to draw a clear line that personal use of business email is prohibited. There are a number of reasons why this is tempting. A business may have concerns about email use related to:

- employee productivity,
- inappropriate personal behavior that may be associated with the business,
- personal privacy and
- security breaches.

However, most of us recognize that occasionally a personal matter may be discussed via a business email account, so exceptions may apply and policies on how to handle personal email may be practical and appropriate.

The American Bar Association offers this language as an example of how to discuss personal use in a company email policy:
"...incidental and occasional brief personal use is permitted within reasonable limits, so long as it does not interfere with the employee's work."

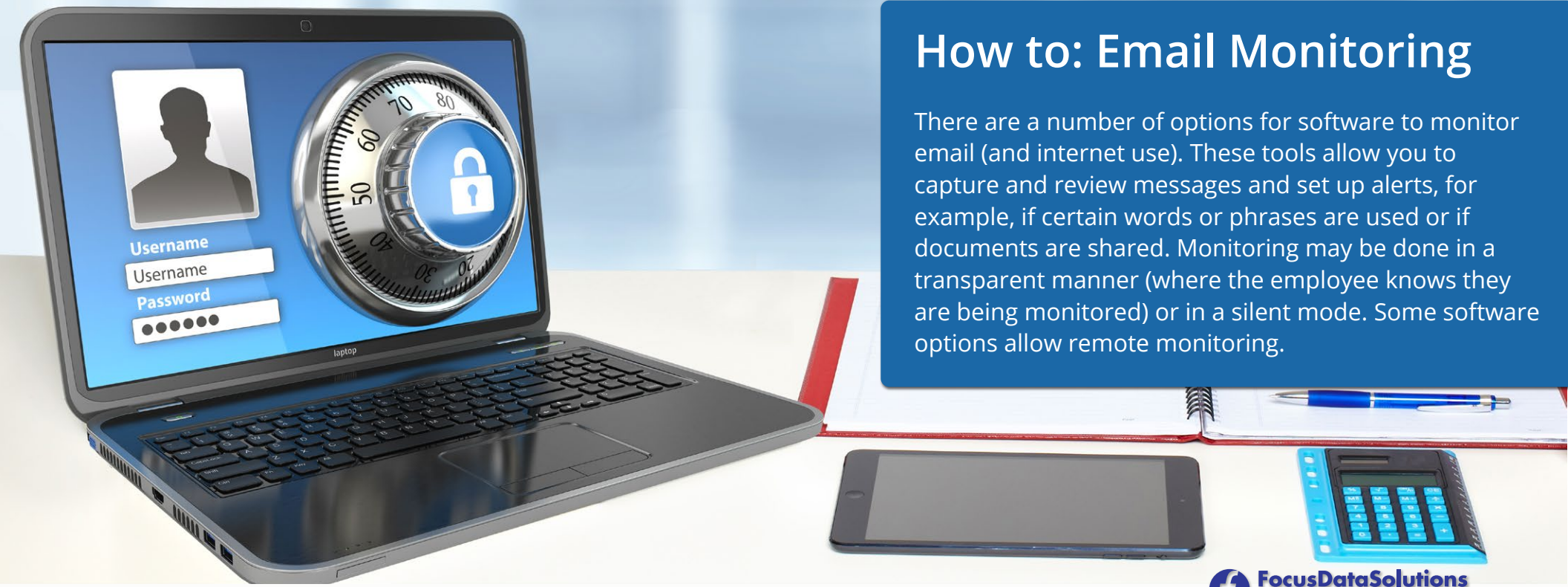
A more specific policy may:

- limit the amount of time or hours during which employees may communicate personal messages (e.g., breaks or lunch),
- require that personal emails are saved in a separate folder,
- prohibit the opening of attachments in personal emails,
- prohibit the use of business email to sign up for accounts not related to business (e.g., online promotions, newsletters, etc.).

2 Company Property

Following the principle of "business email is for business use," it is important to be clear that company email is the company's property. As such, employees should be made aware that:

- There should be no expectation of privacy where company email is concerned, even if personal in nature. In other words, anything that is sent, received, created or stored on a company's computer system may be viewed.
- Emails are part of the company's records and may be subject to discovery in a legal case.
- The employer may monitor employees' use of email (it is legally important to make employees aware of potential monitoring).



How to: Email Monitoring

There are a number of options for software to monitor email (and internet use). These tools allow you to capture and review messages and set up alerts, for example, if certain words or phrases are used or if documents are shared. Monitoring may be done in a transparent manner (where the employee knows they are being monitored) or in a silent mode. Some software options allow remote monitoring.

3 What is NOT Allowed

In the interest of heading off bad or even illegal behavior and protecting the company from liability, it is worthwhile to be explicit about what types of communications are prohibited by company policy. For example, email sent via the company's system:

- may not be used to harass or make threats, nor be offensive or disruptive in nature;
- may not include language or images related to race, gender, age, sexual orientation; pornography, religious or political beliefs, national origin, or disability;
- may not present personal views as the company's own;
- may not engage in commercial activity unrelated to the company;
- may not distribute copyrighted material; and
- may not share confidential material, trade secrets, or proprietary information outside of the company.

4 Receipt of Inappropriate Email

Employees should be encouraged to report the receipt of any inappropriate email with prohibited content to a supervisor or manager.

The company should put a protocol in place to investigate and address any reports of inappropriate email in a timely manner.

5 Company and Network Security

Email may provide a window for security breaches. Phishing and more specifically spear phishing emails have increased and are common cyberattacks on small businesses. Phishing refers to emails that appear to come from a legitimate source but are scams designed to steal private, sensitive information. In 2015, 43 percent of phishing campaigns were targeted at small businesses (Symantec). An estimated 91% of cyberattacks start with phishing (PhishMe). Therefore, it is important to make employees aware of security threats through training and enforce smart email protocols as part of a company's policies. Some simple rules may include:

- Be suspicious of unknown links or requests sent through email or text message.
- Do not open email attachments from unknown sources, and only open attachments from known sources after confirming the sender.
- Never click on links in emails.
- Do not respond to requests for personal or sensitive information via email, even if the request appears to be from a trusted source.
- Verify the authenticity of requests from companies or individuals by contacting them directly.
- Any proprietary or sensitive information sent via email should be encrypted.

6 Retention

To the extent that a company has document retention policies, email policies should explain what should be retained, where and for how long. Different industries and businesses may be subject to different regulatory standards that should be considered.

7 Etiquette

In addition to telling employees what not to do, an email policy provides an opportunity to discuss preferred protocols in communications. Even if etiquette is not included as part of a formal policy, businesses may wish to provide tips to employees related to:

- Professionalism – Emails should be professional and respectful in tone -- err on the side of formal vs. casual.
- Spelling/grammar – Spell check should be enabled and grammar checked before sending emails.
- Proofread – Before sending, employees should re-read their emails to correct errors, check tone and avoid miscommunication.
- Address – Add the email recipient's address after composing the email to avoid sending an unfinished/unedited message. Double check the recipients' addresses before sending.
- Signature – Employees may be asked to include specific information as part of their signature (website address, phone number, social media links, or disclaimers).
- Reply all – To respect others' time and inbox capacity, limit replies to those who need to know the information being conveyed.
- Forward – It's probably best not to forward without permission, or at least to review all content that will be forwarded to avoid sending sensitive information. Do not alter others' text.
- Capitalization – Avoid using ALL CAPS in email communications.
- Turnaround/response – Employees are expected to respond to emails both internally and externally within a reasonable (or set) timeframe.

8 Quality of Work and Life

Technology has dramatically improved the speed by which we can do business, but it can be abused. Depending on industry demands and a company's culture, it may make sense to set some parameters around email use to limit the intrusion technology can pose, both on personal lives and productivity. Companies may adopt policies that:

- limit the use of email after hours,
- limit email during vacations,
- limit the use of internal email (i.e., make colleagues talk to each other),
- limit use of email during certain work hours (dedicated "off-line" hours).

9 Consequences of Noncompliance

To encourage compliance with company policies, there should be enforcement. Employees should know the consequences of breaching the email policy, including disciplinary action up to and including termination.

10 Acknowledgement

To ensure that employees are aware of the company policy on email use, it needs to be readily available to them. The policy may be in the employee handbook, posted on the company intranet, or stored in a public folder. It is always helpful to have training and discussions around company policy, and employees may be required to sign an acknowledgement that they have reviewed and understand the rules and expectations.

In Summary

Email is an important business tool to facilitate communication and workplace efficiency. However, misuse can translate into legal trouble, reputational harm and security breaches. A thoughtful email policy tailored to your business can maximize email as a tool and avoid the undesirable consequences of poor judgement by employees. By setting clear guidelines about appropriate, ill-advised and unacceptable email practice, a business can gain peace of mind and a more productive workplace.

FocusDataSolutions

Focus Data Solutions is a technology company that works with a wide array of clients in Northern Virginia and the DC metro area to fulfill their technology needs. From 24/7 monitoring and service, network security and preventative maintenance, to web and email hosting, network relocation, backup and disaster recovery, FDS offers the IT services companies need to meet their business goals. Focus Data Solutions seeks client relationships that include a commitment to communication, collaboration and trust -- the guiding principles of FDS service.

1020 N. Fairfax Street, Suite 400 | Alexandria, VA 22314 | 703-836-0080 | www.focusdatasolutions.com