Business Email:
Navigating the Legal Minefield

LORMAN®

Published on www.lorman.com - November 2017

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Business Email: Navigating the Legal Minefield

With the advances in technology, employees can chat with other employees and clients in an instantaneous session, check their social media status and add updates, transmit company secrets and spread information to millions of people in only a few seconds. Billions of emails are sent every day, posing potential problems for employers and employees. While email provides an effective form of communication, it can also plant legal mines and put the business at risk. Before creating your business email policy, take full consideration of the factors that affect your business and the benefits of establishing a clear business email policy. Next, begin to draft your email policy to work for you and your employees.

Potential Legal Problems Associated with Business Email

While you probably hope to use business email to increase efficiency and provide a shorthand for document retention, having business email can come with a litany of legal problems. For example, one study in 2003 reports that about one out of ever twenty employers fights a claim of sexual harassment or workplace discrimination based on employees' email and Internet use. Some high-profile cases have resulted in millions or billions' of dollars in damages when employees sent inappropriate emails to other employees.

Sometimes having business email is risky because it creates a legal document. One 2003 study reports that 14 percent of workplace email is subpoenaed by the courts. Today, that number may be even higher. Federal and state rules of civil procedure also allow parties to request electronically-stored data as part of the discovery process. Any wrongdoing on the employer's side may easily be proven by looking to this electronic data. However, some businesses are subjected to mandatory retention policies in which they must keep certain information for a specific period of time and they must comply with these rules.

Other legal problems may arise due to the use of business email. For example, an employee may violate a client's confidentiality by forwarding confidential information. Another employee may send inappropriate emails to colleagues. Being proactive about the business email policy can help employers avoid these types of problems.

Reasons to Develop Guidelines for Business Email Use

Most companies monitor their employees' Internet connections, including their email. In fact, the American Management Association cites that more than 75 percent of companies in the United States monitor their employee's online use. Out of these companies, about 80 percent of them inform their employees that they are tracking their Internet use and monitoring their emails. Even though most employees are aware that their bosses are monitoring their use, the amount of personal use of email in the workplace is continuing to go up. In fact, approximately 60 percent of employees who access the Internet while working actually admit to using the Internet and email for their own personal reasons. These statistics indicate that employees are accustomed to using their employers' Internet and email for their own social reasons and that they are in need of concrete guidelines to modify their behavior.

Electronic liabilities may be reduced if an employer actively creates and notifies employees in writing about a business email policy. While some states legally require employers to notify employees of monitoring their email and Internet use, it is still a good idea for most companies to notify employees regardless of the mandate of law of the business email policy. Notification may curb inappropriate behavior and provide a defense in case an employee later challenges the monitoring of the account due to privacy concerns or of a dismissal when he or she violates the policy.

Additionally, notifying employees that an employer plans to monitor their email can help the employer modify his or her own policy. He or she may not actively monitor emails, but notification protects his or her right to do so in the future in case suspicious activity occurs or if the employer is investigating an employee for sexual harassment or other misconduct.

Elron Software completed a survey in 1999 and found that 60 percent of employees admitted to sending or receiving personal email that was adult-oriented at work. Additionally, the survey found that 55 percent of workers admitted to receiving email messages that were sexist, racist or otherwise offensive, and 10 percent of employees admitted to sending confidential information about other companies in email. Having a business email policy can help employers specify their expectations for employee conduct and provide appropriate procedures for handling an employee who violates the policy.

Items to Include in Your Business Email Policy

Every business email policy is different because the type of business and needs of the business are different. However, there are some general parameters that employers may wish to consider including in their business email policies, including the following:

Personal use of email - Let your employees know whether or not you permit them to use business email for transmitting or receiving messages. You may wish to prohibit these types of messages. However, you may want to consider how realistic this is and whether you really want to enforce it. For example, are you willing to punish an employee for sending his wife a happy birthday e-card? If you have restrictions about personal email, specify those restrictions. For example, discuss the hours when employees can send these messages, the number of messages that they can send, whether or not they can send attachments, etc.

Right to monitor - Explain to employees that you have the right to monitor their business email use at any time, regardless of the item that was used to send or receive the email. If an employee uses company equipment to send or receive messages on email, their communications are not private. Additionally, employers may have the right to monitor emails sent on the business email even if the employee transmits the message on a personal cell phone or laptop.

Method of monitoring - If you have decided to use a particular system to monitor employee email or Internet use, include this information in the business email policy. For example, you may use a program that keeps track of keystrokes or one that flags certain words and then copies the message. Clearly explain the system. However, if you have not decided on your method of monitoring business email exchanges, include possible ways that you may monitor the email system, but use language that allows for other methods to be used in the future.

Rules - Employers should make clear any rules that employees should adhere to. These rules may include the following topics:

Anti-harassment - employees should be made aware of the prohibition of transmitting inappropriate or offensive messages, images or content. Ideally, the business email policy should reference an anti-discrimination policy that is already in place.

Conduct - an employee who uses a business email is representing the business. For this reason, all emails should be formatted in a professional manner with a professional representation of the company.

Confidentiality - remind employees that trade secrets, confidentiality agreements and non-disclosure agreements still apply to business email communication.

Netiquette - you may want to provide details about how employees should send emails, such as by requiring them to use salutations, a closing signature with his or her name, title, address, telephone number and email address. Employers may also want to ensure that emails are grammatically correct and may recommend that employees use grammar check feature.

Best practices - The email use policy may include suggestions that can help protect employees and employers. For example, it may require encrypting messages or providing a confidentiality notice on certain emails. It may also suggest that employees keep passwords private and not written down. In an effort to save space, the email policy may also request that employees delete emails that are not considered records.

Prohibited Use - Provide a specific list of prohibited actions. For example, you may want to emphasize that business use may not be used to transmit messages, links, images or content that is threatening, obscene, harassing or offensive. You may also want to specify that business email cannot be used to make defamatory or libelous statements about anyone. Other restrictions may include prohibiting employees from emailing software programs, videos, links to videos or programs or audio files if these items are not relevant to the job. Software programs or other products of this nature may be excluded from being sent or received if doing so would violate licensing agreements in place. There may also be special parameters regarding accessing business email while the employee is not at work. He or she may need special permission from his or her department head to access this account. Additionally, employers may wish to exclude employees from accessing personal email accounts while using company equipment or on company time. Finally, the employer may wish to specify that business email accounts should not be made to complete or advance any illegal or unethical activities.

Retention policy - Employers may have a specific retention policy of records that is based on the particular type of business and the needs of the business. However, there may be additional requirements for certain types of governmental entities, non-profit organizations or other types of businesses regarding document and electronic data retention. Businesses must comply with these policies. A retention policy may request that employees delete email after a specific period of time in order to avoid storage problems. For example, the employer may ask that this task be completed after 30 days. Employers may install an automated system that will automatically delete messages after a certain period of time. The policy should also specify how important emails should be saved to avoid this purge. A different amount of days may be appropriate for emails that are considered email, part of Listservs, informational in nature and confidential records. Some employers may wish to consult with a data retention company in order to determine regulatory guidelines with which they must comply, as well as suggestions for establishing clearly defined policies regarding the retention and disposal of electronic documents. Reducing the size of employee mailboxes is one effective way in which a company can prevent employees from using up too much storage space on the email system. Employers may also utilize certain software that allows them or administrators to automatically delete employees' delete or trash folders.

Records handling - Employers may also want to specify how certain emails are handled. This process could be important to keep documents safe and secured. It could also help during a potential lawsuit by having an active policy in place regarding the safe-keeping of records. For example, the policy may ask employees to immediately delete emails that aren't part of the employer's Records Retention Policy. Employees may also be asked to file emails that are important records in a certain manner that is specified by the company. For example, employees may have an electronic file folder that has each client's name on it. The employee may need to place the email in this folder so that the employee and other individuals will be able to access the information at a later date. The company may have other requirements for titling, such as adding the date and type of information to the title. Employees may be asked to move active files to an archived folder.

Safe Handling - The business email policy may also instruct employees about safe handling procedures. For example, it may specify that employees avoid opening attachments unless they are expecting them because viruses may be transmitted in this manner. A virus may cause an employee to inadvertently send private or confidential information to several outside sources, which could affect the business' reputation and liability. Employees may also be instructed to run an anti-virus program that is run by an IT department. In addition to protecting employees and employers from viruses, safe-handling procedures may help to properly safeguard data from accidentally getting lost or destroyed. Employees may be advised to save important emails and attachments to a backup device or drive that is regularly backed up on the business' server. Employers may also tell employees to log off of computers if they will be away from their desks.

Modification of rules - The policy should also specify how the policy may change in the future. This is particularly important as time goes by and more technologies are advanced. Modifying the policy may be completed as employers and employees collaborate to design and implement new policies.

Specification of disciplinary action - Any employee policy that does not specify potential punishments for violating it has no teeth. Employees should know how violating the employee policy may affect their job. If they may be held liable in a civil cause of action, they should also be made aware of this.

Glossary - At the end of a business email policy, there should be a glossary. This glossary should clearly define any terms that may be subject to multiple meanings, as well as general terms that are relied upon in

Special Considerations

In order to ensure that the business email policy is adhered to and that it fulfills all legal requirements, employers should make the policy a collaborative effort by employees and employers. Employers should welcome the input of employees and then clearly communicate this policy to employees. These employees should have a clear understanding of any potential liability associated with not complying or abusing the policy.

Additionally, the policy should be made in a manner that takes the needs of the business together. The employee should not look upon the policy as a restriction of his or her rights, but rather as an instrument that will protect the employee's best interests. The policy should ideally provide for the responsible use of the email system.

However, employees should be reminded that emails and other electronic documents may be used in a lawsuit. For this reason, employees should be reminded that they should not save emails on a hard drive as these are generally subject to legal review.

Employers may also wish to include a team of individuals who will ensure that this policy is successfully developed, implemented and enforced. This team may consist of one or more individuals who utilize technological tools to safely monitor business email systems and people skills so that employees do not feel isolated or violated. Purchasing risk management software may also provide some assistance with this matter.

Another important consideration is to keep passwords secure. Employees should be made to understand that business email accounts often have confidential information inside of them that should not be disseminated to disgruntled clients, former co-workers or competitors. Access to business passwords may also result in malicious individuals stealing data or funds from the company, leading to more legal problems and legal fees for the company. Specific password policies may be included as part of the business email policy. One method to protect passwords is to require passwords to be changed every quarter. Business email may be terminated if an employee's relationship has dissolved with the company. Employers should have a list of each employee's password and this information should be kept in a secure location. Employees should also keep their passwords in secured locations, not on a sticky note by their computer or in an unlocked drawer. Passwords should also be avoided that include personal information. Instead, employees should use a unique combination of letters, punctuation marks and numbers. Employees may also create a system in which employees will have to log back on and enter passwords after being away from a computer for a short period of time.

Employers should ensure that each employee is aware of the business email policy and that he or she receives a copy of the policy. Employees should also be required to consent to the policy, and the signed consent forms should be kept in a safe location in case there is any violation of the policy. Having documented evidence will go a long way in case a legal problem arises.

Investigating Behavior

Having a policy in place is the first step in preventing violations of the policy. However, some employees may violate the policy. If an employee is suspected of behaving in an inappropriate manner, the employer can take several actions to investigate the behavior and protect his or her legal interests. For example, an IT employee may conduct periodic reviews to ensure that employees are not attaching storage devices to computers that are not authorized. The IT department may also be able to conduct routine audits. This step may help employers discover inappropriate language, harassing conduct or personal use of the business email system. Filtering and monitoring software can assist in this regard. If any violating behavior is found, refer to the business email policy to determine the next appropriate steps to take.

Conclusion

When employees do not appropriately use the Internet and business email, they can create substantial legal problems for employers. Employees may transmit messages with harassing or offensive conduct that can land the employee or employer in the middle of a workplace harassment suit. Disgruntled employees may send confidential information to the business' competitors or to their private email accounts. Emails that should have been thrown away may provide the basis of a lawsuit. Additionally, not mentioning that employees are being monitored by their employer may result in the need for employers to defend themselves against civil actions regarding the invasion of privacy. Employees may also be less productive and involved in their work if they are permitted to use business email in an abusive manner. However, a business owner may be able to create a well-defined business email policy that allows employees to have the advantages of this quick method of communication, while also protecting the business owner's legal interests, as well as promoting the employees' responsible use of Internet and business email.