



Exemplar of Company Email Policy

To be used in conjunction with "Email and the Attorney Work Product and Attorney-Client Privilege" webinar presented on September 22, 2010 by David Sasseville of Lindquist & Vennum PLLP and Sarah Stroebel of U.S. Bank.

Email is an important form of internal and external communication. Emails are written records that may be required to be disclosed in legal proceedings or otherwise made public. The Company's ethical standards apply to every email you create – no matter how informal its intent. An email should never be created or sent if it does not first pass the scrutiny of the Company's ethical standards. Even though email is an indispensable form of internal communication, it should not take the place of direct conversations where possible. People communicate better and more efficiently when discussing matters directly, and direct conversations create the opportunity to build better working relationships with each other. While this discussion provides guidance specifically regarding email communications, it also applies in principle to all other forms of communication as well, including voicemail and memos.

All emails should be created with the understanding that they may be formal records and should be written in a professional tone. The transmission of all messages must comply with all policies and be protected from unauthorized disclosure or access. Follow these basic rules when using email:

- Use email within the specific requirements of your job.
- Write email as you would any other letter that may become a formal, written record. Be respectful, clear, truthful, and accurate. Do not exaggerate or use colorful or profane language.
- Do not make disparaging remarks. Avoid writing email in the form of casual conversation.
- Ensure that messages written in response to other messages contain sufficient context to avoid misinterpretation.
- Ensure that your email communications are consistent with the spirit and intent of the Company's ethical standards and policies.
- Never send an email that you would be embarrassed to see repeated in print at a later date.

The standards for safeguarding information and information security also apply to email communications. Because email messages sent outside the Company via public networks, such as the Internet, may be intercepted or misdirected, you must take great care not to include information that may be used to harm the Company, its customers, its employees, or any of its other stakeholders.

When business needs require that you communicate with external parties using email containing Company Confidential or Customer Confidential information, the email must be sent using the Company's secure (encrypted) email facility using the prescribed encryption function. If you are uncertain how to employ the Company's e-mail encryption tools please contact the Company's Information Services department.

Q I need to send an email outside of the company to one of my vendors that contains Company and/or Customer Confidential Information. Can I go ahead and send it?

A Before sending the Company's or Customer's Confidential Information to someone, make sure that you know to whom you are sending it, and make sure the receiver is authorized to receive the information. Ensure you have the correct email address. Limit the information you send to only what the authorized receiver needs to complete the task or request. Don't send information the receiver should already have such as sensitive account or personal information. If you must email Company or Customer Confidential Information to non-Company, external email addresses, activate Secure Mail by selecting the "Send Secure button or by entering the prescribed encryption code into the "Subject" line of the email.

If a customer emails a service request containing personal information or account numbers, remove this information from your email reply. This will reduce the risk of exposure of the Company Customer Confidential information.

The Company may assign workspace, equipment or other Company property for use in performing your job responsibilities. As previously described under this section of the handbook, *Company Resources*, while Company property is intended to be used for Company business, employees may make occasional, inconsequential personal use of the Company's systems, provided that such use does not interfere with business use, consume system resources, or violate any Company policy.

Q Sometimes I need to fax information to my child's school. Is it okay to use a Company fax machine?

A Occasional personal use of a Company fax machine is okay, as long as the number of pages is not excessive and the time to transmit the fax does not unduly interfere with business. If you are unsure, check with your manager.

There is no expectation of privacy in employee use of Company resources and systems, and the Company reserves the right to access and search workspace and equipment that has been assigned to employees and to conduct reasonable surveillance of activities on company premises based on business needs, subject to applicable law. The Company also reserves the right, subject to applicable law, to monitor electronic records of activities associated with usage of employees' systems accounts (user IDs); such usage includes electronic forms of communication (email, telephones, voicemail, and other communications systems), other computer systems, and any other electronic records for any reason.

Equipment owned by employees but used for Company business purposes is not considered private and may be accessed and searched for any purpose, subject to applicable law. Email may be monitored for any reason, including when it appears that use of a system violates criminal or civil law, violates Company policy, or may have an adverse effect on the Company or its employees. Examples include, but are not limited to, emails containing sexual innuendo or other inappropriate or offensive jokes; chain letters; downloading, copying or sending confidential information to an unauthorized party; excessive or unauthorized personal use that violates Company policy; or other use that may be harmful to the Company or its stakeholders.

Q I have heard that my email and Internet access are being monitored. Is that true?

A Email and Internet access are property of the Company and may be monitored. The unauthorized transmission of Company data, access to inappropriate Internet sites, and the transmission of inappropriate emails are examples of misuse of technology, which creates risk for the organization. The misuse of Company resources, including technology, may result in disciplinary action, including termination.