

White paper

Email disclaimers The legal and practical issues



Email disclaimers

The legal and practical issues

Introduction

Email is an essential business tool that not many companies that can do without. However, after several high profile lawsuits with multi-million dollar penalties concerning the contents of corporate emails, companies are increasingly aware that simply by using email they are exposing themselves to a number of legal threats.

One of the ways in which to minimize these legal risks is to add a disclaimer to every email that is sent on or from the company network. This paper discusses why email disclaimers are needed, the different types of disclaimers and how to add them.

'E-mails should be prefaced in such a way as to incorporate the employer's standard terms and conditions'. - Robin Bynoe, Charles Russell Solicitors.

What are email disclaimers?

Email disclaimers are statements that are added to emails to disclaim liability. The statements are usually of a legal character but can also be used for marketing purposes.

'If you are in any doubt as to whether or not you should include a notice, then you should include one'. - Email@work 2000, Jonathan Whelan

Why do you need email disclaimers?

There are three main reasons why you might decide to add disclaimers to your emails: legal protection, regulatory compliance and marketing purposes.

Legal protection

If you were to be so unlucky to be sued for the contents of an email, it is not certain whether an email disclaimer will protect you from liability in a court of law. However, it can help your case and in some situations might exempt you from liability. More importantly, it may well prevent the actual occurrence of lawsuits against your company since the mere presence of the statement might deter most persons from seeking legal compensation from your company. Besides avoiding liability, disclaimers are also used to prevent persons from unlawfully forwarding or copying

confidential emails. Again, the presence of the notice will deter most persons from doing this. Therefore the use of disclaimers is always recommended.

'The disclaimers added to the end of emails are not legally binding, but it's always good practice to try and disclaim liability'. - Michael Chissick, Head of Internet law at Field Fisher Waterhouse.

There are 6 legal threats that disclaimers can help protect against:

- **Breach of confidentiality**

By including a disclaimer that warns that the content of the email is confidential, you can help protect your company against the exposure of confidential information. If the receiver breaches this confidentiality, they could be liable.

- **Accidental breach of confidentiality**

If an employee were to receive a confidential mail from someone and by accident forward it to an unauthorized person, the employee, and therefore the company, could be held liable. This can happen for instance if a wrongly addressed email is forwarded to a postmaster, who might not be authorized to read the mail, or if an email message is intercepted. If you include a statement at the end of your mail that the email is only intended for the addressee and that if anyone receives the email by mistake they are bound to confidentiality, this could protect you.

- **Transmission of viruses**

If an employee sends or forwards an email that contains a virus, your company can be sued for this. Apart from implementing a good virus checker that blocks viruses entering and leaving the company via email, you can also warn in your disclaimer that the email can possibly contain viruses and that the receiver is responsible for checking and deleting viruses.

- **Entering into contracts**

Written communication, including email, can be used to form binding legal contracts if the individuals have actual or apparent authority to do so. If you do not wish certain employees to be able to form binding contracts by email, you could include a statement that any form of contract needs to be confirmed by the person's manager.

*'In the early days of the electronic telegraph, a gun dealer in the USA telegraphed a message to a potential buyer saying: 'I have thirty rifles to sell at \$10 each.' The buyer wanted to buy 3 rifles and telegraphed 'I will buy th[re]e rifles'. But the message got corrupted, 'three rifles' became 'the rifles', and the dealer dispatched all thirty rifles. The court ruled that the buyer had contracted to buy all thirty'. - *Email@work 2000, Jonathan Whelan**

- **Negligent misstatement**

By law, a person is obliged to take care when giving advice that a third party relies on. If an employee were to give professional advice in an email, the company will be liable for the effect of the advice that the recipient or even third

party, reasonably relies upon. A suitable disclaimer could protect your company from this kind of liability.

- **Employer's liability**

Although a company is ultimately responsible for the actions of its employees, including the content of any emails they send, a disclaimer can decrease liability; if a company can show that it has correctly instructed its employees not to send libelous, offensive, obscene or defamatory statements this could help in disclaiming responsibility if an employee breaches these rules. A company can demonstrate this by including an email disclaimer to that effect, and by implementing an email policy that clearly warns employees against misuse of email. However, there is no disclaimer that can protect against actual libelous, offensive or obscene content. The most a disclaimer can accomplish in this respect is to reduce the responsibility of the company, since it can prove that the company has acted responsibly and done everything in its power to stop employees from committing these offenses.

'Defamation, unintended contract formation, misdirected emails all bring into focus the desirability of email disclaimers'. - Simon Halberstam, Specher Grier Halberstam & Co.

Regulatory compliance

New and existing regulations are forcing companies to protect their client's privacy. In the US, the Health Insurance Portability and Accountability Act (HIPAA) requires health care institutions to keep a record of their email communications and secure confidentiality of information. The U.S. Securities and Exchange Commission (SEC) and Gramm-Leach-Bliley Act (GLBA) impose similar duties on financial institutions. Steep penalties can apply to those organizations that do not comply with their industry's regulations.

Therefore in certain industries, organizations are actually required to add disclaimers to their emails in order to protect the integrity of their patients or clients and avoid any confidentiality breaches.

Marketing purposes

A foot note can also be added to serve marketing purposes. Disclaimers can include a company address, URL and/or slogan if wished.

What are the different types of disclaimers?

Disclaimers can be prepended or appended, applied company wide or per department/user, added to external and/or internal mails, and can be static or individualized.

Append or Prepend disclaimers?

If you prepend the disclaimer, there is more chance that it will be read. However, it might interfere more with your email communications. The choice whether to

prepend or append disclaimers will probably depend on how secure and confidential your email communications need to be and how important email is to your company. A legal company or financial institution for instance might choose to prepend disclaimers. However, a company selling books or flowers over the Internet would probably prefer to append the disclaimer. It is also possible to place a short text at the top with a link to the full disclaimer at the bottom of the mail.

Company wide or user/departmental disclaimers

Although a company wide disclaimer might be sufficient for a number of organizations, if at all possible it is advisable to add different disclaimers per business group or department. For instance a person in the sales department might need a statement saying that all quotes are only valid for 30 days. The accounts department might need a disclaimer that concentrates more on the confidential nature of the information. The technical support group might want to include a notice that they cannot be held liable for the consequences of their advice. By adjusting the contents of the disclaimer according to the context, the strength of the notice can be increased.

Internal and/or external mail?

Many companies only add disclaimers to externally sent mails since they are not as aware of the legal implications of internal emails as they are of external emails. Although the virus and contract issues mainly apply to external mails, the confidentiality and employer's liability issues are just as important for internal mail as they are for external mail. For instance, there have been several cases where employees filed hostile work environment claims after being confronted with offensive emails circulating the office. As for confidentiality, this might even be more of an issue for internal mail, since not only is there quite a good chance that a colleague might accidentally read a confidential email, an insider will recognize the importance of the information much faster than an outsider. Preferably the internal disclaimer is different from the external disclaimer, focusing more on the internal confidentiality and hostile work environment issues and for instance including a link to the company's email policy.

Static or individualized disclaimers

A static disclaimer text can be added to emails, or a disclaimer can change according to the context to make the disclaimer statement more specific. Where possible, it would be advisable to be more specific since this might add to the weight of the statement. For instance, instead of saying 'the company will not accept liability', it is better to mention the actual company name: 'Company XYZ will not accept liability'. Furthermore, you could use merge fields in your disclaimers, such as:

- **Recipient name**

If you can include the recipient name in your disclaimer, e.g. 'This email and its contents are only intended for [Mr.X]', this will make it even more clear to whom the email is addressed and that if any other person were to read the information they are bound to confidentiality.

- **Supervisor's name**

In the case of limiting the entering into binding contracts via email, you could mention the name of the supervisor who needs to confirm a contract in writing. For example: 'This employee is not authorized to conclude any binding contracts without the express written confirmation by [Mr. Y]'.

- **Date**

It might also be useful to include a date in the disclaimer.

How can you add disclaimers?

You can add disclaimers to your emails by making use of a signature, or by adding disclaimers at server level. Signatures can be configured in email client software, such as Microsoft Outlook. However, since this is client based the user could change the signature without the employer knowing. Moreover, if you wish to change the signature, you will need to change this on every machine individually. Therefore adding disclaimers at server level is preferred.

Policy Patrol is an email filtering product that can add disclaimers at server level and provides companies with a sophisticated tool for implementing a well-planned disclaimer strategy. By offering user based disclaimers and differentiating between internal and external mails, Policy Patrol allows companies to add different disclaimers in different situations and therefore increase the effectiveness of the disclaimer notice.

Moreover, Policy Patrol includes features that many other products do not offer, such as merge fields and support for formatting (HTML and rich text formats). These features make the disclaimer notices more specific and distinguishable, and thus further improve their strength. Policy Patrol also includes the option to prepend or append disclaimers.

Why choose Policy Patrol?

Compared to other email security products, Policy Patrol is an extremely comprehensive and flexible email filtering solution that offers the following disclaimer features:

- ✓ Policy Patrol offers formatted disclaimers including tables and images and disclaimers as plain text attachment.
- ✓ The program allows you to add a disclaimer for all users or to add different disclaimers for specific users or groups (and optionally select excluded users).
- ✓ Policy Patrol can avoid multiple disclaimers when replying or forwarding, putting an end to the long string of disclaimers at the end of emails.
- ✓ Policy Patrol can merge user fields from Active Directory, Exchange 5.5 or Lotus Domino to personalize a disclaimer or signature.
- ✓ Policy Patrol can append or prepend disclaimers but can also add disclaimers or signatures after the last entered message text. The program also allows you to add a disclaimer at the top of the message with a link to the disclaimer at the bottom of the message.
- ✓ Policy Patrol can add a different disclaimer depending on certain conditions, e.g. a code in the subject, a particular sender or recipient, the existence of an attachment.
- ✓ Policy Patrol is one of the very few products that can add disclaimers to internal mails if installed on Exchange 2000/2003. Furthermore. the program can apply

different disclaimers depending on whether the message is sent internally or externally.

- ✓ Policy Patrol includes the option of sending a blind copy of sent emails to a mailbox for archiving. These mails can then be used to prove that a disclaimer was sent.
- ✓ Scalable: Policy Patrol is available with different feature sets (disclaimers only, with/without anti-virus) and features/users can be added at a later stage according to the customer's needs.
- ✓ User licensing: Policy Patrol only requires the users for whom rules are configured to be licensed.
- ✓ Easy to configure and install. Rules wizard uses Outlook rule wizard logic, making it instantly comprehensible.

Sample disclaimers

Disclaimers can be made up out of statements covering different aspects. Below are some sample statements that can be used for each aspect independently. To make up your disclaimer, select applicable statements and include these in your disclaimer.

▪ **Breach of confidentiality & accidental breach of confidentiality**

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager.

This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system.

If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

▪ **Transmission of viruses**

WARNING: Computer viruses can be transmitted via email. The recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.

Email transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of email transmission.

- **Entering into contracts**

No employee or agent is authorized to conclude any binding agreement on behalf of [Company] with another party by email without express written confirmation by [Supervisor or Director].

- **Negligent misstatement**

Our company accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing.

If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

- **Employer's liability**

Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company.

Employees of [Company] are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by email communications. Any such communication is contrary to company policy and outside the scope of the employment of the individual concerned. The company will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising.

- **Complete disclaimers**

This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. Email transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of email transmission. If verification is required please request a hard-copy version.

This message is confidential. It may also be privileged or otherwise protected by work product immunity or other legal rules. If you have received it by mistake, please let us know by e-mail reply and delete it from your system; you may not copy this message or disclose its contents to anyone. Please send us by fax any message containing deadlines as incoming e-mails are not screened for response deadlines. The integrity and security of this message cannot be guaranteed on the Internet.

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.

Sample departmental disclaimers

Below are some samples of departmental disclaimers and an internal disclaimer.

▪ **Financial department**

The financial department may face more confidentiality issues than other departments:

This message contains confidential information and is intended only for [recipient name]. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately if you have received this e-mail by mistake and delete this e-mail from your system. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email. [Date]

Company X, Suite# 1, Street, City, Country, www.company.com

▪ **Sales department**

The sales department disclaimer must cover the validity of quotes and disclaim responsibility for any action taken in reliance upon information given.

All quotes from [Company] are valid for 30 days following the date of email transmission. The company's standard terms & conditions apply to all orders. Our company accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing. Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email. [Date]

▪ **IT department**

The IT department or helpdesk must disclaim against responsibility for the effects of their advice. For instance if they were to advise a user to change something on their computer and the user does not implement this correctly causing system down time, the company does not want to be held liable for this:

Our company accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information

provided, unless that information is subsequently confirmed in writing. Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. WARNING: Computer viruses can be transmitted via email. The recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email. [Date]

▪ **Secretarial department**

You could include a statement for secretaries that they are acting on behalf of their manager and that the manager must confirm any agreements in emails in writing.

This message is sent of behalf of [Manager] and is intended for [Recipient]. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. [Company] accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing by [Manager]. [Date]

▪ **Board of Directors**

Directors will mainly face confidentiality issues:

This message contains confidential information and is intended for [Recipient]. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission. If verification is required please request a hard-copy version. [Date]

Company X, Suite# 1, Street, City, Country, www.company.com

▪ **Internal disclaimer**

An internal disclaimer is mainly important for disclaiming against libelous, indecent, and racist content in emails, creating a hostile work environment. If employees use the internal email system to spread pornographic pictures or offensive jokes the company will be held liable. Therefore the internal disclaimer should disclaim against this. Confidentiality is also an issue for internal mail.

* This message is intended only for [recipient name]. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

* Employees of [Company] are expressly required not to make defamatory statements and not to infringe or authorize any infringement of

copyright or any other legal right by email communications. Any such communication is contrary to company policy and outside the scope of the employment of the individual concerned. The company will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising. Employees who receive such an email must notify their supervisor immediately. Please visit our intranet for a copy of [Company]'s [email policy](#).

[Date], Company X, Suite# 1, Street, City, Country.

Conclusion

It is a fact that, simply by using email, your company is exposing itself to legal threats. Since prevention is better than the cure (and less expensive), it is important that you take steps in which to minimize the threats. The first step is to draft a company wide email policy and distribute this amongst your employees. The next step is to make sure that the email policy is enforced. Adding legal disclaimers at the bottom of each corporate email will provide the first basic protection against a number of legal issues arising out of the use of email. Furthermore, to further minimize the threat of employer's liability and breach of confidentiality, you should consider using a content filtering tool to block inappropriate and unwanted emails, dangerous attachments and scan messages for viruses.

About Red Earth Software

Red Earth Software is a Microsoft Certified Partner that specializes in the development of content security solutions that help companies ensure proper usage of their email and Internet systems. Policy Patrol currently filters emails for more than 250,000 users worldwide and is used by customers in nearly every industry including educational, non-profit, financial, legal, health care, manufacturing and government. Included among Red Earth Software clients are large international organizations such as Nissan, Targus, Canadian Pacific Railway, USA.net, Lotto, Fujitsu Services (Central Government customer) and Daewoo.

Contacting Red Earth Software

Red Earth Software LLC
200 Marcy Street
Portsmouth, NH 03801
United States
Phone: (603) 436-1319
Fax: (603) 457-8455
Sales: sales@redearthsoftware.com
Support: support@redearthsoftware.com

Red Earth Software (UK) Ltd
20 Market Place
Kingston-upon-Thames
Surrey KT1 1JP

United Kingdom
Tel: +44-(0)20-8605 9074
Fax: +44-(0)20-8605 9075
Sales: sales@reearthsoftware.co.uk
Support: support@reearthsoftware.co.uk

More information

- ⇒ For more information about Policy Patrol or to download a 30-day evaluation version, please visit <http://www.reearthsoftware.com>.
- ⇒ For Red Earth Software's white paper *Email content security - Addressing the email risks*, please go to <http://www.policypatrol.com/Requestwpfrm.htm>.
- ⇒ More articles and white papers by Red Earth Software can be downloaded from <http://www.reearthsoftware.com/download.htm>.

Disclaimer

The contents of this white paper do not constitute legal advice and should not be relied upon as such. If you need legal advice on a specific matter, please contact a lawyer.

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001-2003 by Red Earth Software®.